Escroquerie en matière de virements frauduleux

L'escroquerie au Président

Comment se prémunir contre de telles fraudes ?
Comment protéger les fonds de son entreprise ?

SPUERKEESS

SPUERKEESS.LU

Introduction

Ce guide a pour but de sensibiliser et d'aider les responsables d'entreprises à se prémunir contre un type d'escroquerie en matière de virements frauduleux, communément appelé « escroquerie/fraude/arnaque au Président ». Cette escroquerie jouit d'une popularité croissante à l'étranger mais aussi au Luxembourg.

Dans ce type d'escroquerie, les voleurs réussissent à s'emparer de fonds d'une entreprise en manipulant des employés de l'entreprise de manière à les amener à effectuer des transferts de fonds non souhaités par l'entreprise mais légitimes vis-à-vis de la banque.

L'arnaque se déroule en deux temps :

- les escrocs collectent d'abord des informations sur l'entreprise, son fonctionnement interne et son personnel. Sur base des éléments récoltés, ils élaborent un stratagème plus ou moins sophistiqué pour piéger des employés et déjouer les mécanismes de validation et de contrôle de l'entreprise ;
- ils déroulent ensuite le scénario de manipulation proprement dit et amènent des employés clés à initier, valider et signer des paiements non souhaités par l'entreprise, mais légitimes vis-à-vis de la banque.

Les escrocs, souvent très bien éduqués, ont recours à l'ingénierie sociale*, au piratage informatique, aux ressources technologiques, à l'espionnage et à la dissimulation pour arriver à leur fin.

* L'ingénierie sociale est une méthode de manipulation, qui consiste à utiliser la crédulité de la victime pour obtenir des informations personnelles et confidentielles sous de faux prétextes. Ce processus, utilisé contre les employés, notamment ceux des organisations où sont détenus des actifs ou des informations sensibles, repose sur l'établissement d'une relation de confiance inappropriée.

Les fraudeurs

En règle générale, l'arnaque est organisée par un groupe d'escrocs :

- très bien organisés ;
- éduqués ;
- maîtrisant de multiples compétences, tels l'ingénierie sociale, la gestion d'entreprise, la finance, la comptabilité, le droit des sociétés ;
- spécialistes en matière de technologies de l'information et de la communication ;
- à l'aise dans les langues véhiculaires ;
- capables d'**adapter leur stratégie** en fonction des aléas.

Les cibles

Les entreprises ciblées sont souvent des structures :

- dont l'organisation **et la hiérarchie sont complexes,** voire dispersées sur plusieurs pays ;
- qui ont recours à un **réseau important de partenaires** (avocats, fournisseurs, sous-traitants, ...) ;
- dont la direction et l'entité ciblée sont géographiquement séparées, avec peu de contact direct entre les exécutants et le(s) dirigeant(s).

L'entreprise peut être plus vulnérable lorsqu'elle se retrouve en **situation exceptionnelle** (contraintes financières, risque d'OPA, projet d'importance capitale, changement de direction, ...).

Les employés ciblés sont ceux qui touchent de près ou de loin à la chaîne financière :

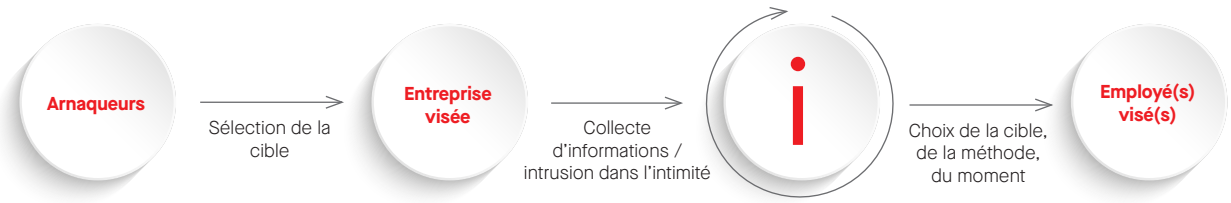
- des **cadres de niveau hiérarchique moyen ou élevé** ;
- des **employés** administratifs ;
- des membres des services de **comptabilité** ;
- toute autre personne ayant un **accès à la trésorerie ou à des comptes de l'entreprise ou de clients**.

Les ordres de virement seront en effet valablement initiés, validés et signés par un ou plusieurs employés/cadres de l'entreprise ayant accès aux fonds.

L'arnaque

1 - La préparation

Après avoir choisi une cible potentielle, les fraudeurs apprennent à connaitre l'entreprise, trouvent une ou plusieurs failles dans son fonctionnement et élaborent la stratégie d'attaque. Cette phase peut comprendre des **recherches intensives** et des observations de **longue durée** qui peuvent s'étendre sur plusieurs mois. Les escrocs cherchent à obtenir des **informations sensibles** sur les personnes, l'organisation, la structure, les procédures internes, voire la culture de l'entreprise. Tous les moyens, légaux et illégaux, sont bons pour obtenir les informations recherchées.



Exemples de sources librement accessibles :

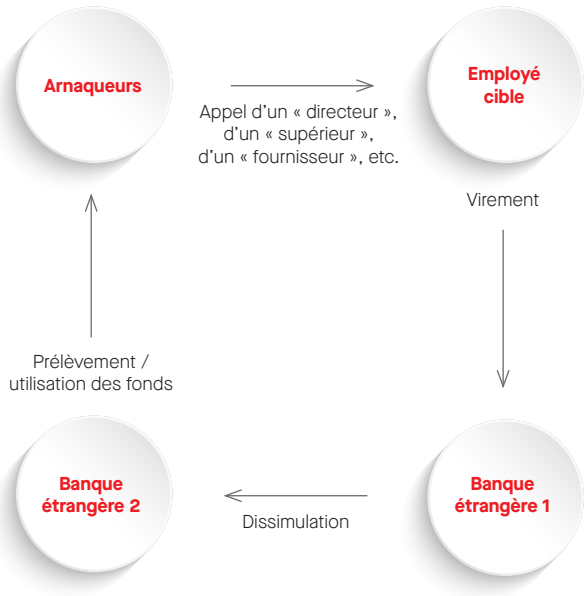
- site internet (structure, organisation, fonctionnement, hiérarchie, projets en cours, rapports, bilans, numéros de comptes), articles, interviews, statuts ;
- achat d'informations via des sites spécialisés en intelligence économique comme societe.com, infogreffe.fr ou hoovers.com ;
- collecte de données à travers les réseaux sociaux (Linkedin, Facebook, X, Instagram, Snapchat, etc.).

Intrusion dans l'intimité de l'entreprise :

- prises de contact sous de faux prétextes, faux e-mails ou faux documents : usurpation d'identité ou de qualité (cadre, collègue d'une autre entité, investisseur, client, fournisseur, faux questionnaires ou enquêtes, avocat, investisseur, etc.) ;
- questions anodines de nature à récolter des informations supplémentaires (« Est-ce que M. XY est là ? » « Non, il est en congé de maladie pendant un mois. Il est remplacé par Mme.... ») ;
- menaces (licenciement si refus de fournir des informations) ;
- flatterie, promesses de faveurs, promotion (pour obtenir des informations).

2 - Le passage à l'acte

Le moment venu, le ou les employés ciblés sont contactés afin d'être amenés à initier des paiements, à modifier le numéro de compte d'un ordre permanent ou d'un bénéficiaire enregistré. On leur donne l'impression d'avoir affaire à **une autorité « hiérarchique » ou « légitimée » ayant un lien avec l'entreprise** et on leur présente un contexte exceptionnel (urgence, confidentialité, chantage, flatterie, promesse) pour les « forcer » à négliger ou contourner les procédures internes et suivre les instructions frauduleuses.



Ordre : effectuer un virement ou modifier le numéro de compte d'un bénéficiaire, d'urgence et en toute discrétion, en faveur d'un compte situé en principe à l'étranger.

Motif : une opération importante en cours.

Assurances : envoi de faux documents, appel d'un deuxième arnaqueur jouant le rôle d'un autre « cadre supérieur » de l'entreprise ou d'un avocat. Renforcement de la crédibilité en invoquant un vocabulaire et des détails internes (services, noms, projets) qu'un externe n'est pas censé connaître.

Menaces : licenciement ou faillite de l'entreprise entière, autorité persuasive.

Situation : vacances, chef(s) en congé, entreprise en situation exceptionnelle, projet important en cours, ...

Afin de contourner des contrôles internes, les ordres sont en général à initier personnellement, utilisant un canal habituel pour communiquer avec la banque de la société.

Très souvent, ces ordres sont qualifiés d' « urgents » et « discrets » dans le cadre d'une **« opération importante en cours »**. Il n'est pas exclu que le projet ou l'opération mentionnée **existe effectivement** et que l'arnaqueur en ait pris connaissance (la victime par contre **n'en est souvent pas suffisamment informée**).

Le moment **peut** être choisi **méticuleusement** (vacances, week-end, jour férié ou pont, chef en congé ou malade, entreprise en situation exceptionnelle, etc.).

Les signes d'alarme

Les situations ou indications suivantes doivent susciter la suspicion et déclencher une vigilance accrue

A. L'employé est contacté directement par

- un **supérieur hiérarchique** qu'il ne connaît **pas personnellement** ;
- un responsable d'une filiale étrangère qu'il ne connaît pas personnellement ;
- une personne de type leader, directeur, fils du directeur, responsable, actionnaire principal, fournisseur important, notaire ou toute autre **personne qui n'aurait aucune raison de le contacter directement**.

B. Toute instruction

- caractérisée comme urgente sous un prétexte quelconque (de manière à ce que l'employé contacté ne puisse pas vérifier le bien-fondé) ;
- caractérisée comme discrète pour des raisons quelconques et/ou non vérifiables directement (de manière à ce que l'employé contacté ne puisse pas alerter son supérieur) ;
- qualifiée comme étant **cruciale pour la survie de l'entreprise** (éviter la faillite de l'entreprise, l'échec d'un projet en cours, une OPA en cours, ...) ;
- vers une **banque située à l'étranger ou à l'extérieur de l'UE** sous un prétexte quelconque (ex: Europe de l'Est, Asie) ;
- qui est **contraire aux procédures internes**.

C. Autres indications

- une personne **essaie d'intimider** et se réfère à son autorité ou à sa position importante en rapport avec l'entreprise (que l'employé contacté ne peut pas vérifier) ;
- l'équipe est en **sous-effectif** (jours fériés, vacances, etc.) et/ou les **supérieurs directs** sont **absents** respectivement **injoignables** ;
- la personne ne **veut** ou ne **peut pas** laisser ses **coordonnées précises** sous un prétexte quelconque (empêchant de clarifier son identité) ;
- appels et/ou e-mails depuis des numéros/adresses **inconnus, suspects** ou **masqués**.

Prevention et comportement

Mesures préventives

Limiter toute divulgation/publication vers l'extérieur (tant au niveau privé que professionnel) d'informations **générales ou sensibles**, même celles de moindre importance, liées aux procédures, à l'organisation, au fonctionnement ou bien aux projets internes de l'entreprise. Une attention particulière doit être conférée aux réseaux sociaux (Linkedin, Facebook, X, Instagram, Snapchat, etc.).

Former et **informer** le personnel de l'entreprise qui a accès aux comptes bancaires des différents risques de fraude.

Avoir des **procédures précises et rigoureuses** en matière d'initiation, de validation et de signature de virements bancaires ainsi qu'en matière de changement de références bancaires au niveau des systèmes de l'entreprise (compte fournisseur, etc.).

Que faire en cas de signe(s) d'alarme(s) ?

Inviter l'interlocuteur téléphonique ou l'expéditeur du mail à suivre les procédures en vigueur et à utiliser un canal de communication sécurisé (ex. mail interne ou professionnel). Refuser tout autre moyen et **ne pas se laisser intimider**.

Toujours vérifier le bien-fondé de la demande et se **poser la question** : est-il **logique** que **« telle » personne** me contacte **directement** ? Au moindre doute : contacter sans délai un supérieur hiérarchique, un autre responsable ou au moins un autre collègue. S'il s'agit d'un prétendu partenaire externe, essayer de le contacter directement pour confirmation (recherche du numéro dans l'annuaire téléphonique). **Ne jamais procéder à la demande sans la consultation d'autres personnes.**

Vérifier l'exactitude des adresses e-mail : parfois les usurpateurs ajoutent ou changent seulement une lettre ou un signe (ex.: directeur@spuerkeesss.lu, dirigeant@votreentreprise-.lu etc.). Elle doit impérativement et exactement se terminer par le nom de domaine de votre entreprise. Dans certains cas, un nom seul est affiché et l'adresse peut alors être vérifiée au moment du « Reply to ». Au moindre doute, adressez-vous à votre service informatique ou à votre supérieur direct (même si l'expéditeur semble correct alors que le contenu vous semble suspect).

Que faire en cas de doute ?

Aviser immédiatement le supérieur hiérarchique.

Si le doute est confirmé :

- contactez **sans délai** vos banques pour les prévenir ; si des ordres ont déjà été transmis à votre banque, il est peut-être encore possible de les annuler ou de faire bloquer un paiement ; la banque pourra vous conseiller sur la marche à suivre ;
- alertez votre service informatique afin de vérifier et, le cas échéant, de rétablir la sécurité informatique ; le CIRCL (Computer Incident Response Center Luxembourg) pourra être contacté en cas de besoin d'assistance technique ou de conseils.

En resumé

Situation

Le directeur, fournisseur, notaire... etc. de votre entreprise vous contacte...

par téléphone

Pouvez-vous clairement identifier le numéro et/ou la voix ?

Non : méfiance !

Oui

par e-mail

L'adresse e-mail est-elle correcte et sécurisée ?

Non : méfiance !

Oui : vigilance !

par fax

Méfiance !

La sollicitation

- Est-elle qualifiée d'URGENTE et/ou DISCRETE ?
- Vous semble-t-elle incohérente ou étrange ?
- Consiste-t-elle en une opération de paiement / modification de données bancaires ?
- La personne fait-elle de la pression / des menaces (licenciement) ?
- La personne vous demande-t-elle de déroger aux procédures internes ?

Non

Vérifiez le bien-fondé de la demande (en cas de doute : méfiance) !

Au moins 1x oui

MEFIANCE !!!
Ne suivez en aucun cas les instructions sans avoir consulté un supérieur ou une autre personne !

Questions de bon sens

Quelle est la probabilité que cette personne vous contacte directement et personnellement ? Si faible, alors MEFIANCE !

Pourquoi votre directeur aurait-il besoin de vous envoyer un fax ?

Est-ce qu'il aurait une raison de vous envoyer un mail ? Si vous n'êtes pas un cadre supérieur : très improbable !

Même si l'adresse du mail vous semble correcte, le compte, ne pourrait-il pas avoir été piraté ? Vigilance : vérifiez le bien-fondé et la cohérence !

Quelle est la probabilité que votre directeur déroge à ses propres procédures internes ?

Quelle est la probabilité qu'il contacte à cette fin justement une personne qu'il ne connaît pas ?

Ne serait-ce pas un abus de pouvoir ? Risqueriez-vous vraiment un licenciement en cas de refus ?

- Etre **vigilant** par rapport aux informations qui sont divulguées vers l'extérieur.
- Respecter les **procédures internes**, même en situation exceptionnelle.
- Se méfier des notions d'**URGENCE** et de **DISCRETION**.
- Faire preuve de **bon sens** : en cas de méfiance ou de doute, consulter un supérieur direct ou un autre collègue.

Liens utiles

Informations générales au sujet des fraudes :
guichet.lu : https://guichet.public.lu/fr/entreprises/gestion-juridique-comptabilite/contentieux/litiges/arnaques.html
cssf.lu : https://www.cssf.lu/fr/fraude-financiere/

Pour se protéger, prévenir et analyser les cyber-risques :
info@nc3.lu

Pour rapporter ou réagir à un incident cyber :
https://www.circl.lu/report/

Pour un contact avec la Luxembourg House of Cybersecurity et être orienté vers le département qui correspond le mieux à vos besoins :
https://cybersecurity.lu

Pour obtenir une liste d'outils mis à disposition par le CIRCL et le NC3 :
https://circl.lu/services/
https://nc3.lu/

Pour en savoir plus sur le ransomware, attaque la plus fréquente sur les PME :
https://circl.lu/pub/tr-57/

SPUERKEESS

Banque et Caisse d'Epargne de l'Etat, Luxembourg, établissement public autonome
1, Place de Metz, L-1930 Luxembourg, R.C.S. Luxembourg B30775

12/23