



Prévention des escroqueries aux virements internationaux

1- Introduction

Au vu de la recrudescence constatée des escroqueries aux virements internationaux, il y a lieu de sensibiliser les employés sur ces pratiques provoquant parfois un préjudice de plusieurs centaines de milliers € voire de millions €

Ces escroqueries sont toujours précédées d'une « campagne » de recherche d'informations, en général téléphonique, visant à obtenir des renseignements sur le collaborateur susceptible de procéder au virement (son nom, fonction occupée, sa carrière, etc.). Une bonne vigilance à ce stade permet de ne pas communiquer d'informations de nature à faciliter l'escroquerie.

2- Sur la phase de préparation

Ces recherches d'informations sont réalisées au moyen d'une technique communément appelée « ingénierie sociale ». Cette technique consiste pour l'escroc à obtenir des informations sur l'entreprise ciblée -ou l'individu ciblé- par fax, e-mail, téléphone, ou de visu, en usurpant une qualité, en flattant, en prêchant le faux pour savoir le vrai, en menaçant de licenciement, en adressant de faux questionnaires de satisfaction, etc.

La manipulation fonctionne d'autant mieux que son auteur a la capacité d'y aller « au culot ». L'air assuré et entendu arboré ne vous incitera alors pas à remettre en cause sa qualité ou sa démarche.

Ainsi, l'escroquerie est toujours précédée d'une phase de recueil de renseignement sur l'entreprise ciblée, afin de permettre à l'auteur, ainsi documenté, de pouvoir se faire passer pour un membre de votre cercle le jour où il sollicitera le virement bancaire. Sa faculté d'élocution, alliée à la connaissance de votre entreprise, lui permettra alors de gagner votre confiance.

3- Signaux qui doivent éveiller votre méfiance :

Les escroqueries constatées par la DCRI ont pour points communs :

- a-** l'usurpation d'identité de responsables de votre groupe (fondateur, P-DG, fils du P-DG, directeur financier, directeur marketing, etc.), de manière à intimider l'employé à qui il est demandé de faire le virement ;
- b-** un caractère d'urgence est avancé sous un prétexte quelconque (afin de ne pas laisser le temps de vérifier le bien-fondé de la demande de virement) ;
- c-** une totale discrétion est requise sous un prétexte quelconque (afin de ne pas alerter un responsable hiérarchique qui pourrait détecter l'escroquerie) ;
- d-** la demande de virement se fait au profit d'une banque généralement située hors de l'Union européenne, de manière à compliquer l'entraide judiciaire ;
- e-** les victimes sont majoritairement -mais pas exclusivement- des employés de filiales étrangères de groupes français ;
- f-** ces escroqueries sont -en particulier, mais pas exclusivement- commises lorsqu'un weekend est suivi -ou précédé- d'un jour férié ou d'un pont engendré par un jour férié (ce délai permet de retarder la découverte du virement indu) ;
- e-** enfin, l'auteur de la supercherie prétextera le plus souvent être en déplacement pour ne pas laisser de coordonnées vérifiables.

4- La bonne démarche consiste à :

a- avant l'escroquerie : vérifier s'il existe des procédures internes sur les virements, si ces procédures sont connues et si elles sont appliquées (contre-appel sur une ligne fixe, vérification que l'e-mail provient bien de la société (attention au nom de domaine), double signature requise au-delà d'un certain montant, etc. ;

Faire une communication interne vers les équipes financières et comptables pour les sensibiliser, ainsi qu'à l'attention d'un personnel plus large : tout employé exerçant une fonction de « filtre » = secrétaires, assistantes de direction, standardistes, etc. Ce personnel est en effet susceptible d'être contacté par l'escroc pour obtenir des informations sur votre entreprise dans le cadre de la phase préparatoire (recueil d'informations sur la cible).

Ne pas rendre public, sur votre site Internet, votre organigramme. La possession de ce document interne est de nature à faciliter les repérages de l'escroc.

b- pendant l'escroquerie : en cas de demande de virement faite hors formalisme habituel, exiger une demande écrite provenant d'une adresse mail professionnelle (et non personnelle), ainsi qu'un numéro de téléphone fixe (et non portable). Orienter votre interlocuteur vers la procédure régulière, et ne rien entreprendre sans aval hiérarchique.

c- après l'escroquerie : déposer plainte auprès de la « section financière » du Service Régional de Police Judiciaire (SRPJ) de votre ressort ;

Par ailleurs, et éventuellement, afin de faciliter le travail de la police, il peut être utile de se prêter provisoirement au jeu avec l'escroc, en feignant une collaboration, afin de récupérer des informations.

Enfin, il a été constaté que, lorsque ces manœuvres échouent et que la supercherie n'a pas été détectée, l'échec est dû à la seconde signature requise pour les virements bancaires dépassant un certain montant.

Dans de petites structures où employés et dirigeants se connaissent bien, la supercherie a pu échouer, car l'employé ciblé n'a pas reconnu la voix de son prétendu patron, ou parce que ce dernier prétendait appeler du siège français, alors que l'employé ciblé savait qu'au même moment son patron était en déplacement à l'étranger.

5- En résumé

La prévention de ces escroqueries passe par le bon sens des personnes ciblées :

- au regard de votre position dans l'entreprise, serait-il logique que votre PDG vous appelle, vous personnellement, pour solliciter un virement ?
- est-il logique que votre P-DG vous incite à déroger au formalisme en vigueur pour procéder à un virement bancaire ? Dans tous les cas :

**Retenez que les notions de
discrétion et d'urgence prétextées
doivent impérativement éveiller votre suspicion !**