Prévention des escroqueries aux faux ordres de virements internationaux (FOVI)

Depuis 2010, plusieurs milliers d'escroqueries ou tentatives d'escroqueries aux faux ordres de virements internationaux visent des sociétés implantées en France et/ou filiales domiciliées à l'étranger. Ces escroqueries ont généré un préjudice global d'environ 890 millions d'Euros pour les faits commis et plus de 1,8 milliard d'euros pour les faits tentés.

Réalisée par téléphone et/ou par mail, l'escroquerie concerne les sociétés quelles que soient leurs tailles. Souvent situés à l'étranger, les escrocs collectent un maximum de renseignements sur l'entreprise (ingénierie sociale sur internet) avant de lancer leur opération sur les personnes capables d'opérer ces virements.

I. Les variantes de l'escroquerie :

Ces modes opératoires ne sont pas exhaustifs. Les escrocs les renouvellent régulièrement.

L'escroquerie « au faux président » :
Usurpant l'identité du dirigeant ou d'un responsable de la société ciblée, les malfaiteurs prennent contact avec le service comptabilité et, sollicitant la plus grande confidentialité concernant un projet de fusion/acquisition à l'étranger ou l'imminence d'un contrôle fiscal, transmettent un RIB d'un compte à l'étranger et font ainsi indûment virer des fonds.

Indices pouvant alerter *:*
Un Email évoquant un rachat de sociétés, une demande de la DGFIP, un contrôle fiscal, etc...
L'appel d'un tiers usurpant l'identité d'un cabinet d'avocats, d'un conseiller juridique, etc...
L'urgence de la situation,
Le secret et la confidentialité mentionnés dans la conversation,
La flatterie ou l'intimidation.

L'escroquerie « au changement de Relevé d'Identité Bancaire » :
Un escroc simule un changement de domiciliation bancaire du bailleur, d'un fournisseur ou de tout autre créancier légitime de l'entreprise pour les prochains règlements de factures, ou détourne le paiement des salaires du personnel par l'utilisation d'un nouveau RIB. Il envoie les nouvelles coordonnées bancaires par courrier électronique, avec des caractéristiques de messagerie très proches de celles de l'interlocuteur habituel.

Indice pouvant alerter *:*
Toute demande de modification de coordonnées ou changement de compte bancaire pour un compte français ou étranger.

L'escroquerie à l'informatique ou au faux technicien :
Apparue en 2013, l'escroquerie dite « au virement SEPA » a été remplacée par une variante consistant à se faire passer pour un faux technicien de l'établissement bancaire qui prend attache avec la victime :
- soit pour lui demander de cliquer sur un lien contenant un «logiciel espion» puis de les inviter à se connecter sur le portail de leur banque gestionnaire (consultation en ligne) et à composer leurs identifiants et leurs codes d'accès. Dès lors, en possession des codes d'accès internet et des exemplaires portant les identifiants de la société, les auteurs confectionnent des faux ordres de virement, les transmettent aux banques et modifient les mots de passe d'accès aux services en ligne privant les services comptables de toute possibilité de vérification de leur trésorerie.
- soit pour l'assister sur l'application bancaire en ligne et l'inciter à réaliser des virements bancaires sur un compte fourni par l'escroc.

Indices pouvant alerter *:*
Un interlocuteur propose une assistance sur les outils de paiement,
Des questions d'un interlocuteur sur les outils et/ou processus de paiement,
Une demande de connexion par l'intermédiaire d'un hyperlien,
Une demande de virement test.

Pour se prémunir de toutes ces formes d'escroqueries, il suffit de mettre en œuvre des mesures simples de sécurité pour décourager les escrocs. Il est également important de sensibiliser et de former vos personnels à la détection de ce type d'arnaques.

II) Les signes d'une attaque :

Un virement à l'international non planifié est demandé par un membre du conseil d'administration, le dirigeant, l'un de ses adjoints, avec l'aide d'un cabinet d'avocats, sous la surveillance de l'Autorité des Marchés Financiers, par l'un « des fournisseurs » prétextant un changement de coordonnées bancaires. Cette demande peut revêtir un caractère urgent et confidentiel. L'escroc fera usage de flatterie ou de menace dans le but de manipuler son interlocuteur.
Pour asseoir sa crédibilité et usurper une fonction, l'escroc apportera une abondance de détails sur l'entreprise et son environnement : données personnelles concernant le chef de l'entreprise, ses collaborateurs, les banques, etc...
Un fournisseur vous appelle et vous indique que sa comptabilité a été délocalisée. Les factures seront dorénavant à régler sur un nouveau compte bancaire en France ou à l'étranger.

III) Se prémunir d'une attaque :

Résister aux tentatives d'intimidation et à la pression psychologique.
En cas de doute, prendre attache directement avec la personne au sein de la société soit physiquement soit avec les coordonnées connues de l'entreprise.
Se méfier de tout changement de coordonnées téléphoniques ou mails : la communication d'un nouveau numéro à l'indicatif français n'est pas une garantie, tout comme une adresse mail hébergée par un opérateur généraliste. Dans ce dernier cas, l'affichage complet de l'entête du mail permettra d'identifier le réel émetteur.

Désigner un nombre restreint de personnes autorisées à valider les modifications de coordonnées bancaires et téléphoniques.

IV) Exécution du virement :

Effectuer en urgence un compte rendu de l'événement à la hiérarchie.

Contacter immédiatement votre chargé d'affaires afin qu'un retour des fonds soit effectué dans les plus brefs délais.

MINISTÈRE DE L'INTÉRIEUR
Liberté Égalité Fraternité

Déposer plainte en apportant un maximum d'éléments (entête de mails et leurs contenus, numéros de téléphone utilisés par les escrocs, dates et heures des appels, les éléments confidentiels communiqués aux escroc, etc...).

V) La prévention :

1°) Ne pas communiquer d'informations susceptibles de faciliter le travail des escrocs :

Les noms des différents managers, chefs de division, des personnes en charge des paiements fournisseurs, et leurs absences ou congés,
Les techniques de règlement (chèques, virements, prélèvements, etc...), les noms des applications employées dans les processus de règlement, les codes d'exécution des virements,
Le listing de tout ou partie des fournisseurs, des clients, et / ou des duplicatas de factures.

2°) Prendre le temps de vérifier les éléments :

Les escrocs invoquent souvent un caractère d'urgence à leur demande de virement. Il est d'autant plus nécessaire de prendre le temps d'effectuer des vérifications, a fortiori si l'opération demandée est inhabituelle.
Cette vérification peut par exemple prendre la forme :
- d'un contre-appel auprès du partenaire commercial ou financier au moyen de coordonnées figurant dans les fichiers internes de l'entreprise (ligne de téléphone fixe par exemple),
- d'une consultation de factures antérieures en cas de « rappel de transmission de duplicatas de factures »,

- d'une demande de renseignement auprès de ses collègues ou de sa hiérarchie.

Attention : Toute opération prétendument urgente doit être systématiquement présentée au responsable hiérarchique désigné, particulièrement celle qui exigerait la discrétion.

3°) Faire preuve de bon sens et s'interroger sur toute demande inhabituelle, illogique, différente des procédures définies par la société.

4°) Sensibiliser le personnel susceptible d'être contacté par les escrocs mais également les fournisseurs et les clients :

Le service comptabilité, les fournisseurs, la trésorerie, les secrétaires et standardistes.
Effectuer des formations de sensibilisation en interne.
Deux E learning sont à disposition des entreprises, l'un pour l'escroquerie au faux président, l'autre pour l'escroquerie au changement de coordonnées bancaires :

Pour l'accès au module E-learning de prévention de l'arnaque au faux président :
Version web pour visualisation en ligne : http://www.ccampuslearn.net/TRANSIT/CDSE/2012746_we_14/story.html

Version web téléchargement : http://www.ccampuslearn.net/TRANSIT/CDSE/2012746_we_14.zip

Version exécutable en local sur un PC ou diffusion via clé USB : http://www.ccampuslearn.net/TRANSIT/CDSE/2012746_cd_14.zip

Pour l'accès au module E-learning de prévention de l'escroquerie au changement de coordonnées bancaires :
https://www.lesclesdelabanque.com/Anti_fraude_FR_EN_web/story_html5.html

Il est possible d'installer le E learning sur une plate-forme dans une entreprise, il suffit d'adresser une demande au Club des Directeurs de Sécurité et de Sûreté des Entreprises (CDSE) : secretariat@cdse.fr

Pour une connaissance plus globale sur les risques de fraudes et de cybercriminalité, vous pouvez consulter différents sites :
https://www.lesclesdelabanque.com/
https://www.ssi.gouv.fr/

5°) Veiller à la sécurité des accès aux services de banque à distance :

Les codes d'accès au service de banque à distance de l'entreprise doivent être uniquement connus des personnes habilitées à s'y connecter. Ces codes d'accès doivent rester strictement confidentiels et ne pas être reportés sur un quelconque document ou communiqués à qui que ce soit. Les mots de passe doivent être suffisamment complexes et régulièrement modifiés.
L'établissement bancaire ne vous demandera jamais les informations permettant la connexion à votre espace de banque à distance.

6°) Sécuriser les installations informatiques :

Afin de limiter le risque d'infection et de piratage informatique (par des logiciels espions ou des programmes malveillants), la possibilité d'installation de logiciels sur les ordinateurs doit être strictement encadrée et vos postes informatiques doivent posséder un antivirus régulièrement mis à jour.
Préserver les bases clients et fournisseurs.

Une charte informatique précisant les conditions d'utilisation du matériel informatique de l'entreprise et s'appliquant à l'ensemble des collaborateurs est indiquée et accessible par tout le personnel.

7°) Effectuer une veille sur les évolutions des escroqueries par la presse, les communications des pouvoirs publics, les fédérations, les associations professionnelles.

POLICE
NATIONALE