Intelligence économique

Les questions que votre entreprise doit se poser

. Quelles sont les informations stratégiques que vous ne souhaiteriez pas que votre concurrent connaisse ?

. Ces informations sont-elles protégées matériellement (pièce sécurisée) et virtuellement (cryptage des fichiers) ?

. Quelles sont les personnes qui ont accès à ces informations ?

. Ces personnes ont-elles été sensibilisées aux risques de vol d'information ou de piratage informatique ?

. L'ensemble de votre personnel est-il sensibilisé à la protection de ses données personnelles, notamment sur les réseaux sociaux ?

. Votre service comptabilité est-il sensibilisé aux risques d'escroqueries aux faux ordres de virement ?

. Les sous-traitants, mais aussi fournisseurs et stagiaires font-ils l'objet d'un contrôle particulier ?

. Disposez-vous d'une procédure/protocole de gestion de crise en cas de perte d'informations stratégiques (qui contacter pour déposer plainte, quelle procédure juridique mettre en œuvre, etc.) ?

. Disposez-vous d'un système de veille sur votre e-réputation ? Et sur celle de vos concurrents ?

Ce que dit la loi

L'escroquerie est le fait de tromper une personne physique ou morale afin de l'inciter à remettre des fonds, des valeurs, des services ou un bien quelconque.
Ce délit est puni de 05 ans d'emprisonnement et de 375 000 euros d'amende. La tentative est sanctionnée des mêmes peines.

QUELS SIGNES DOIVENT VOUS ALERTER ?

Un grand nombre d'escroqueries financières comporte des similitudes permettant facilement de les détecter.

Vous retiendriez :
. qu'elles sont souvent commises les veilles de week-ends, et plus particulièrement lorsqu'ils sont suivis ou précédés de jours fériés,

. que les demandes de virement se font à l'international, qu'elles sont non planifiées et qu'elles ont toujours un caractère confidentiel et urgent pour empêcher la victime de vérifier le bien fondé de la sollicitation,

. que l'escroc apporte souvent une abondance de détails sur l'entreprise, qu'il fait usage de flatterie ou de menace dans le but de manipuler la victime, qu'il fait parfois appel à de faux avocats ou de faux policiers,

. qu'aucune coordonnée transmise par l'escroc n'est vérifiable, celui-ci prétextant dans bien des cas être en déplacement et ne pouvoir être contacté autrement que par téléphone portable,

. que les demandes de virement sont souvent faites au profit de banques situées hors Union Européenne (mais pas toujours), de manière à compliquer au maximum le travail des enquêteurs par la suite.

A RETENIR

Les notions de "**CONFIDENTIALITÉ**" et "**D'URGENCE**" doivent immédiatement éveiller vos soupçons.

Votre brigade de gendarmerie locale

SOYEZ ACTEUR DE VOTRE PROPRE SÉCURITÉ

Votre gendarmerie locale communique
GROUPEMENT DE GENDARMERIE DEPARTEMENTALE DES DEUX-SEVRES

Entreprises vigilantes

Je me protège contre les escroqueries aux faux ordres de virement.

La prévention de ce type d'atteinte passe essentiellement par le bon sens des personnes ciblées et l'application stricte des procédures édictées en interne.

RETROUVEZ-NOUS SUR FACEBOOK
gendarmerie.deux.sevres

Une vague d'escroqueries connue sous le nom **d'escroquerie aux faux ordres de virement** a touché récemment plusieurs entreprises du département des Deux-Sèvres, parfois avec un très lourd préjudice.

Réalisée par téléphone ou par courriel, l'escroquerie aux faux ordres de virement concerne les entreprises de toutes tailles et de tous les secteurs.

Opérant souvent depuis l'étranger, bien organisés et informés, jouant sur l'usurpation d'identité, très habiles dans l'art de manier certains ressorts psychologiques, les escrocs abusent leurs victimes sans exercer de violence.

Lancée en direction des services capables d'opérer les virements (comptabilité, trésorerie, secrétariat, etc.) et après avoir récupéré un maximum d'informations sur l'entreprise, **l'opération consiste pour les escrocs à les convaincre d'effectuer en urgence et en toute discrétion un virement important à un tiers sous prétexte d'une dette à régler, de provision de contrat, du paiement d'un loyer, etc.**

Exemples d'escroqueries

L'escroquerie au faux président
L'escroc se fait passer pour le président de la société et exige du comptable un virement express, généralement au moyen d'une fausse facture.

L'escroquerie au loyer
L'escroc contacte le service comptable de l'entreprise et exige que le loyer soit viré en urgence sur le compte d'une société basée à l'étranger.

L'escroquerie au virement SEPA
L'escroc prétexte une série de tests dans le cadre du passage à cette norme en fournissant des coordonnées bancaires domiciliées à l'étranger et en demandant le versement des montants correspondant aux virements tests.

COMMENT S'EN PRÉMUNIR ?

Instaurer des procédures écrites validant à différents niveaux la demande d'un versement vers un compte à l'international. L'objectif est de toujours contrôler l'identité du donneur d'ordre.

Vérifier régulièrement qu'elles sont connues et appliquées par le personnel concerné.

Sensibiliser régulièrement l'ensemble du personnel des services concernés. Ces personnes sont également susceptibles d'être contactées par l'escroc lors de la phase préparatoire de recueil d'informations.

Prendre l'habitude d'en informer systématiquement les remplaçants sur ces postes.

Les former au bon usage des moyens informatiques mis à leur disposition, aux dangers des réseaux sociaux, ainsi qu'à la protection de l'information. Les responsabiliser par la mise en place d'une charte.

Ne pas rendre public l'organigramme de l'entreprise pour ne pas faciliter la collecte d'informations de l'escroc. Filtrer les renseignements mis en ligne sur votre site internet.

Rompre la chaîne des mails pour les courriers se rapportant à des virements internationaux en saisissant soi-même l'adresse habituelle du donneur d'ordre (ne pas utiliser le bouton "Répondre").

Accentuer la vigilance sur les périodes de congés scolaires, les jours fériés et les jours de paiement des loyers.

Maintenir à jour le système de sécurité informatique afin d'éviter toute infection par un logiciel malveillant.

Inviter l'ensemble du personnel à faire rapidement remonter à la hiérarchie tout fait anormal.

DURANT LA PHASE DE "CONTACT"

Lorsqu'une demande de virement est faite hors de la procédure habituelle, exiger une sollicitation écrite provenant d'une adresse courriel professionnelle et un numéro de téléphone fixe.

Suivre scrupuleusement la procédure édictée en interne et ne rien entreprendre sans l'aval de la hiérarchie.

Vérifier systématiquement les coordonnées recueillies.

Ne communiquer aucun code confidentiel par téléphone ou par courriel.

Si une tentative de fraude venait à être détectée durant la phase de contact, tenter de retourner la situation à son avantage en collectant un maximum de renseignements sur l'appelant. Dans le même temps, appeler la gendarmerie nationale.

C'EST TROP TARD, COMMENT FAIRE ?

L'urgence est de bloquer l'argent sur le compte bancaire où il est détenu pour pouvoir ensuite le rapatrier. Pour cela, INFORMER IMMÉDIATEMENT l'établissement bancaire émetteur afin qu'il signale la fraude. Demander à ce que la banque créditrice soit également immédiatement informée des faits.

Informer la gendarmerie nationale et déposer plainte en apportant le maximum d'éléments concernant les ordres de virement, les courriels échangés, etc.

Demander à votre service informatique de conserver les échanges de mails et tenter d'identifier les adresses IP. N'hésitez pas à mandater une société spécialisée pour effectuer cette mission si besoin.