D6. Les escroqueries dites « au président » ou Fovi

Depuis quelques années, les escroqueries aux faux ordres de virement (Fovi), dites également au président, se multiplient, faisant de nombreuses victimes parmi les entreprises. Les services de l'État, les collectivités locales et les établissements publics de santé sont également concernés. Outre le préjudice financier direct, les conséquences peuvent être dramatiques pour la poursuite de l'activité.

Le mode opératoire

Le but d'un Fovi est d'obtenir la réalisation d'un virement, souvent à l'international, au profit de l'escroc. En général, le mode opératoire revêt les caractéristiques suivantes : l'escroc se fait passer pour le président de l'entreprise lors d'un contact téléphonique ou par courriel avec les services comptables ; il crédibilise sa demande et met en confiance la victime grâce à de l'**ingénierie sociale** ; il utilise des ressorts psychologiques visant à abolir le discernement de la victime pour lui faire prendre des décisions sous le coup de l'urgence et de la confidentialité.

Se prémunir

ORGANISATIONNEL

- Sensibiliser régulièrement tout le personnel (y compris les stagiaires, les nouveaux arrivants, les saisonniers, les prestataires, etc.) à ce type d'escroquerie.
- Expliquer les principales vulnérabilités associées à l'usage des réseaux sociaux et la nécessité de ne pas mettre en avant des informations qui pourraient être utilisées dans le cadre d'un Fovi (déplacements de la direction, organigramme trop détaillé, informations comptables, etc.).
- Mettre en place des procédures de vérifications et de signatures multiples pour les paiements internationaux.

TECHNIQUE

- Maintenir à jour le système de sécurité informatique.

COMPORTEMENTAL

- Respecter les procédures mises en place malgré les pressions d'un interlocuteur souhaitant un paiement dans l'urgence.
- Exiger une sollicitation écrite via un courriel professionnel afin de pouvoir la vérifier. Faire de même avec un numéro de téléphone fixe.
- Être attentif aux demandes inhabituelles de transmission de nouvelles coordonnées bancaires et, plus largement, faire remonter toute information jugée inquiétante.
- Redoubler de vigilance sur les périodes de congés scolaires, les jours fériés, les vendredis soir, les week-ends et les périodes de remplacement.
- Se rapprocher de son organisme bancaire et suivre les procédures indiquées.

Conduite à tenir en cas d'escroquerie

COMPORTEMENTAL

➤ Identifier immédiatement les virements exécutés, les mandats de paiement ou les demandes de paiement en instance ou à venir concernés.

➤ Demander le blocage des coordonnées bancaires frauduleuses dans les applications métiers.

➤ Si le paiement n'est pas encore intervenu, suspendre le mandat ou la demande de paiement.

➤ Si le paiement est déjà intervenu, demander le blocage ou le retour des fonds auprès de l'instance bancaire.

➤ Déposer plainte auprès des services de police et de gendarmerie, en apportant un maximum d'éléments (références des virements, coordonnées des personnes contactées). Un dépôt de plainte rapide permet d'optimiser les chances de récupérer les fonds versés.

Escroqueries similaires

➤ **La fraude au « changement de RIB »** : l'escroc s'adresse aux services de comptabilité d'une entreprise en se faisant passer pour un fournisseur. Il demande ensuite le règlement de factures sur un compte bancaire autre que le compte habituel.

➤ **La fraude au « faux technicien »** : l'escroc se présente comme un technicien informatique venant réaliser une opération de maintenance sur l'outil de gestion des comptes et virements.

➤ **La fraude « au faux ministre »** : cette escroquerie consiste à atteindre un dirigeant, en usurpant l'identité d'un ministre, pour le convaincre de virer des fonds à l'étranger en vue de mener des actions de lutte contre le terrorisme ou de libération d'otages.

Mots clés

Ingénierie sociale : recueil d'informations sur une cible basé sur l'étude de l'environnement personnel et/ou professionnel, à partir notamment des informations publiées sur les réseaux sociaux.

Escroquerie : 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 (délit puni de cinq ans d'emprisonnement et de 375 000 € d'amende - article 313-1 du Code pénal).

Pour aller plus loin

➤ Fédération des banques françaises (FBF)
- Consignes de prévention indispensables pour éviter les escroqueries aux faux ordres de virement internationaux (Fovi)

➤ Ministère de l'Intérieur – OCLCTIC (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication)

Portail officiel de signalement des contenus illicites de l'Internet :

https://www.internet-signalement.gouv.fr