A A Imprimer PDF

FOVI : MESURES PRÉVENTIVES

Une recrudescence des faux ordres de virement frappant les entreprises est observée.

Qu'est ce que le FOVI

L'escroquerie aux faux ordres de virement (FOVI) désigne un type d'arnaque qui, par persuasion, menaces ou pressions diverses, vise à amener la victime à réaliser un virement de fonds non planifié.

Parfois présenté comme émanant d'un dirigeant et ayant un caractère « urgent et confidentiel », on parle alors « d'arnaque au Président ».
Une variante consiste à usurper l'identité d'un fournisseur pour communiquer de nouvelles coordonnées bancaires (changement de RIB) sur lesquelles il faut effectuer un règlement.
Une autre variante consiste à usurper l'identité d'un salarié de l'organisation pour demander le changement des coordonnées bancaires où virer son salaire.

Le compte bancaire appartenant à l'escroc est souvent situé à l'étranger. Cette catégorie d'escroquerie est généralement réalisée par téléphone et/ou par messages électroniques, voire les deux, et concerne tous les types d'organisation.

Mesures préventives

Sensibilisez vos collaborateurs et cadres

aux risques notamment de réception de messages frauduleux d'hameçonnage (phishing) visant à leur dérober leurs mots de passe et en particulier si vos services de messagerie sont hébergés ou accessibles en externe.

Diffusez des procédures claires aux collaborateurs

mandatés sur les règles d'authentification des émetteurs et de confirmation des demandes de virement imprévues ou de validation des changements de coordonnées bancaires.

Mettez en place une précdure de vérification

et de validation hiérarchique interne non dérogeable des demandes de virement imprévues ou d'acceptation de changements de coordonnées bancaires.

Veillez à limiter la publication d'informations

(site Internet, réseaux sociaux...) permettant d'identifier et de contacter vos collaborateurs habilités à réaliser des demandes de virement ou des modifications de coordonnées bancaires.

Généralisez l'utilisation des mots de passe

solides pour les comptes de messagerie et activez la double authentification pour limiter les risques de piratage (**conseils pour gérer vos mots de passe**).

Consulter la fiche de l'Assistance et prévention en sécurité informatique.