RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

L'ESCROQUERIE AUX FAUX ORDRES DE VIREMENT (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.

BUT RECHERCHÉ

Escroquerie financière en usurpant l'identité d'un dirigeant, d'un fournisseur ou d'un employé visant à faire verser de l'argent sur un compte bancaire détenu par les cybercriminels. Dans certains cas, cette fraude fait suite au piratage et à l'utilisation de la messagerie de la personne ou entité usurpée.

SI VOUS ÊTES VICTIME

IDENTIFIEZ LES VIREMENTS FRAUDULEUX. Identifiez tous les virements exécutés, en instance ou à venir à destination de l'escroc. Informez votre hiérarchie ainsi que le service comptable et demandez le blocage des coordonnées bancaires frauduleuses dans les applications métiers.

DEMANDEZ LA SUSPENSION DU VIREMENT. Si le virement n'est pas encore effectué, contactez immédiatement votre service comptable pour suspendre la demande de virement frauduleuse.

ALERTEZ IMMÉDIATEMENT VOTRE BANQUE ET DEMANDEZ LE RETOUR DES FONDS. Si le virement a été réalisé, contactez au plus vite votre banque pour demander le retour des fonds. Votre dépôt de plainte pourra être exigé de votre banque pour récupérer les sommes.

CONSERVEZ LES PREUVES et en particulier les numéros de téléphones, les messages reçus, les ordres de virement, les factures et toutes informations qui pourront vous servir pour signaler l'escroquerie aux autorités.

SI LA FRAUDE A PU ÊTRE PERMISE PAR LE PIRATAGE D'UN COMPTE DE MESSAGERIE, CHANGEZ IMMÉDIATEMENT SON MOT DE PASSE. Utilisez des mots de passe différents et complexes pour chaque site et application utilisés (tous nos conseils pour gérer vos mots de passe).

DÉPOSEZ PLAINTE. En parallèle des démarches auprès de votre banque, déposez plainte sans tarder au commissariat de police ou à la gendarmerie dont vous dépendez en fournissant toutes les preuves en votre possession.

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

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION