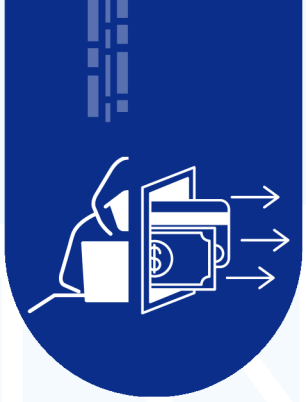
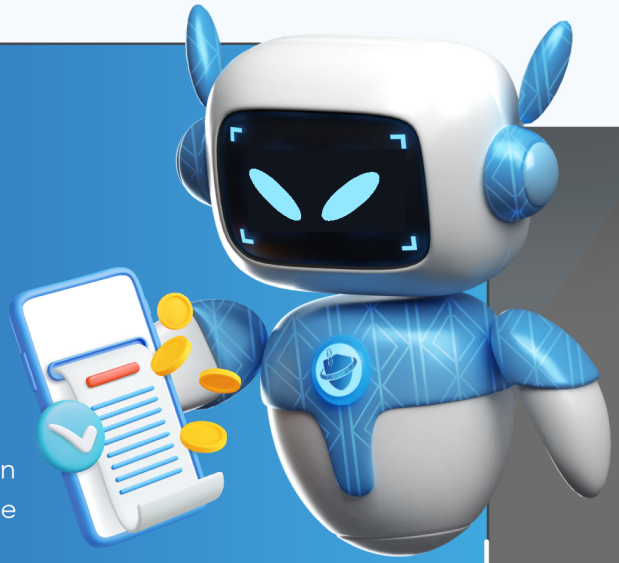


ESCROQUERIE AU FAUX ORDRES DE VIREMENT (FOVI)

CENTRE CYBER DU PACIFIQUE

EN BREF



QU'EST-CE QUE C'EST ?

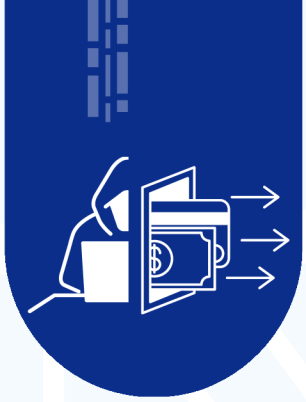
L'escroquerie aux faux ordres de virement (FOVI) consiste à manipuler une victime pour qu'elle effectue un virement non planifié sous pression ou menace. Elle peut usurper l'identité d'un dirigeant (« arnaque au Président »), d'un fournisseur en communiquant de fausses coordonnées bancaires (changement frauduleux de RIB) ou d'un salarié en demandant la modification du compte où verser son salaire. Ces fraudes, souvent réalisées par téléphone ou e-mail, visent toutes les organisations et impliquent des comptes bancaires situés à l'étranger.

BUT RECHERCHÉ : Ces fraudes, souvent réalisées par téléphone ou e-mail, visent à transférer de l'argent sur un compte contrôlé par des cybercriminels.

Voici 6 bonnes pratiques à adopter si vous êtes victime

1. IDENTIFIEZ LES VIREMENTS FRAUDULEUX
2. DEMANDEZ LA SUSPENSION DU VIREMENT
3. ALERTEZ IMMÉDIATEMENT VOTRE BANQUE ET DEMANDEZ LE RETOUR DES FONDS
4. CONSERVEZ LES PREUVES
5. SI LA FRAUDE A PU ÊTRE PERMISE PAR LE PIRATAGE D'UN COMPTE DE MESSAGERIE, CHANGEZ IMMÉDIATEMENT SON MOT DE PASSE
6. DÉPOSEZ PLAINTE

▶ Voir détail page "6 BONNES PRATIQUES À ADOPTER"



ESCROQUERIE AU FAUX ORDRES DE VIREMENT (FOVI)

CENTRE CYBER DU PACIFIQUE

6 BONNES PRATIQUES À ADOPTER

1. 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.

2. 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.

3. 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.

4. CONSERVEZ LES PREUVES

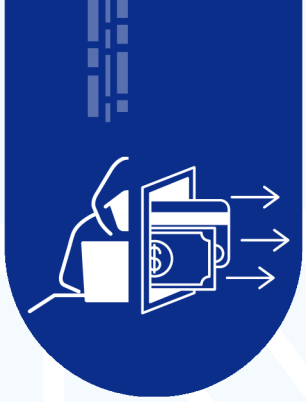
et en particulier les numéros de téléphones, les messages reçus, les ordres de virement, les factures et toutes informations qui pourront vous servir pour signaler l'escroquerie aux autorités.

5. 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).

6. 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.



ESCROQUERIE AU FAUX ORDRES DE VIREMENT (FOVI)

CENTRE CYBER DU PACIFIQUE

COMMENT S'EN PROTÉGER ?

Sensibilisez vos collaborateurs et cadres aux risques :
notamment de réception de messages frauduleux d'hameçonnage (phishing) visant à leur dérober leurs mots de passe, 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 FONCTION DU CAS D'ESPÈCE, LES INFRACTIONS SUIVANTES PEUVENT ÊTRE RETENUES :

• **Escroquerie** (article 313-1 du code pénal). L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. Délit passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende. La tentative d'escroquerie est passible des mêmes peines (article 313-3 du code pénal).

• **Usurpation d'identité** (article 226-4-1 du code pénal). Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est passible d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende. La tentative d'escroquerie est passible des mêmes peines (article 225-5 du code pénal).

• **Accès frauduleux à un système de traitement automatisé de données** (article 323-1 du code pénal). Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de trois ans d'emprisonnement et de 100 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine encourue est de cinq ans d'emprisonnement et de 150 000 euros.
La tentative de cette infraction est punie des mêmes peines (article 323-7 du code pénal).