

## La Police Nationale vous informe

# Commerçants, PME, particuliers, que faire en cas de fraude au virement ou au faux RIB ? Comment se protéger ?

**Tout le monde peut en être victime !!!**

### 1. Qu'est-ce qu'une fraude au virement ou faux RIB ?

L'escroquerie au virement ou arnaque au faux RIB a pour objectif de **tromper la victime, en usurpant l'identité d'un créancier** avec lequel elle est en relation (artisan, notaire, avocat, propriétaire/bailleur...), afin de **lui faire réaliser un virement** vers un compte bancaire détenu par un escroc.

Ce type d'escroquerie est souvent consécutif au piratage d'un compte mail.

Il peut s'agir du compte mail du créancier avec lequel la victime est en relation ou bien de celui de la victime dont l'escroc aura pris le contrôle.

En pratique, l'escroc va identifier une transaction imminente ou récurrente entre le créancier et la victime. En usurpant l'identité du créancier, il va alors adresser un message à la victime lui demandant de réaliser le paiement par virement. En général, l'escroc aura joint à son message une facture avec un RIB falsifié contenant les coordonnées d'un compte bancaire qu'il détient pour dérober le montant du virement.

## **But recherché:**

Détourner un virement de la victime en usurpant l'identité de son créancier

## **2. Comment se protéger d'une fraude au virement ou faux RIB ?**

**Contactez directement votre créancier pour toute demande de virement sur un nouveau RIB reçu par message.**

Si vous recevez un message vous demandant le règlement d'un impayé par virement sur un RIB que vous n'avez jamais utilisé, appelez votre créancier sur son numéro habituel pour lui faire confirmer le message et les coordonnées du RIB reçus.

**Méfiez-vous des messages qui vous incitent à communiquer votre mot de passe de messagerie.**

Vérifiez qu'ils ne vous amènent pas sur un site frauduleux pour vous le dérober. Attention à l'hameçonnage ( phishing) !!! .

### **Utilisez des mots de passe différents et complexes**

pour chaque site et application que vous utilisez et activez la double authentification dès qu'elle est disponible.

### **Utilisez un antivirus:**

pour vous protéger des virus qui pourraient dérober vos mots de passe.

## **3. Que faire si vous êtes victime d'une fraude au virement ou faux RIB ?**

1. **Alertez immédiatement votre banque de l'opération frauduleuse** pour tenter de suspendre le virement si celui-ci n'est pas encore effectué. Dans le cas contraire, demandez le retour des fonds. Votre banque pourra exiger une copie de votre dépôt de plainte pour instruire votre demande.
2. **Alertez au plus vite le créancier dont l'identité a été usurpée.** Dans le cas de la réception d'une fausse facture avec l'usurpation de l'identité d'un créancier, il est possible que l'un de ses comptes de messagerie ait été piraté. En l'informant, il pourra être à même de prendre les mesures

nécessaires (dépôt de plainte, changement de mot de passe, alerte de ses clients...).

3. **Conservez les preuves**, notamment les messages reçus (mails...), les relevés de comptes, les factures ou toutes autres informations qui pourront vous servir pour signaler les faits. Ces éléments pourront constituer des preuves à valeur juridique en cas de procédures ultérieures.
4. **Vérifiez les paramètres de votre messagerie**. Assurez-vous de l'absence de redirection ou de règles de filtrage et, si vous en identifiez, faites des photos ou des captures d'écran avant de les supprimer.
5. **Changez immédiatement votre mot de passe**. Si l'escroquerie a pu être réalisée suite au piratage de votre messagerie, modifiez immédiatement votre mot de passe et choisissez-en un solide. Reportez-vous si nécessaire à notre fiche conseil relative aux mots de passe.
6. **Déposez plainte**. En parallèle des démarches auprès de votre établissement bancaire, déposez plainte auprès des Forces de l'Ordre dont vous dépendez en fournissant toutes les preuves en votre possession. Le dépôt de plainte doit intervenir dans les plus brefs délais suite à l'identification de l'escroquerie.  
Vous pouvez être accompagné gratuitement dans cette démarche par une association de «France Victimes» au 116 006 (appel et service gratuits), numéro d'aide aux victimes du ministère de la Justice. Service ouvert 7 jours sur 7 de 09h00 à 19h00.
7. **Pour plus de conseils, contactez la plateforme Info Escroqueries** du ministère de l'Intérieur au 0 805 805 817 (appel et service gratuits- Service ouvert de 09h00 à 18h30 du lundi au vendredi.)

#### **4. Fraude au virement, que dit la loi ?**

**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 manœuvres 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. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende.

Si l'escroquerie a pu être réalisée par le piratage de la messagerie (mail) de la victime :

• **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.

• **Atteinte au secret des correspondances** ([article 226-15](#) du Code pénal) : infraction passible d'une peine d'emprisonnement d'un an et de 45.000 euros d'amende.

**Source:** [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) - mai 2023 -