RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

# FRAUDE **AU VIREMENT** (FAUX RIB)

COMPRENDRE LES RISQUES

La fraude au virement ou au faux RIB vise à tromper la victime, en usurpant l'identité d'un créancier avec lequel elle est en relation (artisan, notaire, propriétaire…), afin de lui faire réaliser un virement vers un compte bancaire détenu par un escroc.

Ce type d'escroquerie est souvent consécutif au piratage du compte de messagerie (mail) du créancier ou de la victime.

## BUT RECHERCHÉ

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

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.

## SI VOUS ÊTES VICTIME

**ALERTEZ IMMÉDIATEMENT VOTRE BANQUE** pour tenter de suspendre le virement ou demander le retour des fonds.

**ALERTEZ LE CRÉANCIER DONT L'IDENTITÉ A ÉTÉ USURPÉE** car il est possible que l'un de ses comptes de messagerie ait été piraté.

**CONSERVEZ LES PREUVES** (messages reçus, relevés de comptes, factures…) qui pourront vous servir pour signaler les faits.

**VÉRIFIEZ LES PARAMÈTRES DE VOTRE MESSAGERIE** pour vous assurer de l'absence de règles de redirection ou de filtrage, ou encore de connexions inconnues. Si vous en identifiez, faites des photos ou des captures d'écran avant de les supprimer.

**CHANGEZ IMMÉDIATEMENT VOTRE MOT DE PASSE** si l'escroquerie a pu être réalisée suite au piratage de votre messagerie.

**DÉPOSEZ PLAINTE** au commissariat de police ou à la brigade de gendarmerie ou encore par écrit au procureur de la République du tribunal judiciaire dont vous dépendez.

Pour plus de conseils, **CONTACTEZ INFO ESCROQUERIES** au 0 805 805 817 (appel et service gratuits).

## MESURES PRÉVENTIVES

Pour toute demande de virement sur un nouveau RIB reçu par message, **contactez directement votre créancier sur son numéro habituel pour lui faire confirmer le message et les coordonnées du RIB reçus.**

**Méfiez-vous des messages d'hameçonnage 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.

**Utilisez des mots de passe différents et complexes pour chaque site et application que vous utilisez.** Activez la double authentification quand elle est disponible.

**Appliquez de manière régulière et systématique les mises à jour de sécurité** du système, des applications et des logiciels installés sur vos appareils.

**N'installez des applications ou logiciels que depuis les sites ou magasins officiels** au risque de télécharger une version infectée par un virus.

**Utilisez un antivirus** pour vous protéger des virus qui pourraient dérober vos mots de passe.

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

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

## LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues contre leurs auteurs :

- **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.

**RETROUVEZ TOUTES NOS PUBLICATIONS SUR :**
www.cybermalveillance.gouv.fr



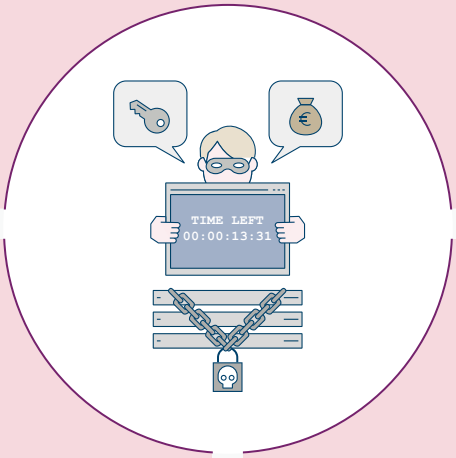
V240201

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

# RANÇONGICIEL
## Vos données sont prises en otage

## QUE SE PASSE-T-IL ?

1. Vos données sont progressivement chiffrées, ce qui les rend inaccessibles




2. L'infection peut s'étendre à tous les appareils connectés au réseau ou aux supports USB branchés

3. On exige de vous le paiement d'une rançon pour récupérer ces données

### Impact de l'attaque

- Intégrité
- Disponibilité
- Confidentialité
- Authenticité

### Motivations principales

- Atteinte à l'image
- Appât du gain
- Revendication
- Espionnage
- Nuisance

## COMMENT RÉAGIR ?
Vous êtes victime d'un rançongiciel
Ne payez pas !

**1 -** Ne pas éteindre la machine concernée
La mettre en veille prolongée si possible

**2 -** Déconnectez immédiatement les appareils du réseau

**3 -** Ne connectez plus aucun appareil sur le réseau

**4 -** Contactez immédiatement votre service informatique ou un expert (ou trouvez le vôtre sur www.cybermalveillance.gouv.fr)

**5 -** Portez plainte auprès des services compétents

## COMMENT SE PROTÉGER ?
Ne tombez pas dans le piège

Effectuez des sauvegardes régulières de vos données

Mettez à jour régulièrement vos principaux logiciels
- Les rançongiciels utilisent les vulnérabilités des programmes pour se propager

Privilégiez un compte utilisateur pour vos usages courants

Courriers électroniques piégés
- Ne faites pas confiance à l'expéditeur de courriers électroniques dont l'origine ou la forme vous semblent douteuses
- Méfiez-vous des pièces jointes et des liens suspects

En savoir plus sur les attaques par rançongiciel :
www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/
www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

Version 2.0 - Janvier 2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION