17 ou 112
@ Brigade Numérique

L'Équipe Prévention Contact de la Compagnie de Gendarmerie de ST OMER vous sensibilise:

Escroquerie au virement / Arnaque au faux RIB

I. Principe

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.
Type d'escroquerie souvent consécutif au piratage du compte de messagerie du créancier ou de la victime.

II. Comment se protéger?

--- Contactez directement votre créancier si vous recevez un message de demande de virement sur un nouveau RIB
--- Méfiez-vous des messages qui vous incitent à communiquer votre mot de passe de messagerie
--- Utilisez des mots de passe différents et complexes
--- Appliquez de manière régulière et systématique les mises à jour de sécurité
--- N'installez des applications ou logiciels que depuis les sites ou magasins officiels
--- Utilisez un antivirus pour vous protéger des virus qui pourraient dérober vos mots de passe.

III. 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**. En cas de 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 toute autre information qui pourront vous servir pour signaler les faits.
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 à un piratage de messagerie., modifiez immédiatement votre mot de passe et choisissez-en un solide.
6. **Déposez plainte,** le plus rapidement possible, en parallèle des démarches « bancaires » au commissariat de police ou à la brigade de gendarmerie dont vous dépendez en fournissant toutes les preuves en votre possession. Vous pouvez être accompagné gratuitement dans cette démarche par une association de France Victimes au 116 006 (appel et service gratuits). Service ouvert 7 jours sur 7 de 9h à 19h.

7. **Liens utiles :**
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-fraude-au-virement-ou-au-faux-rib
https://www.economie.gouv.fr/dgccrf/entrepreneurs-sachez-comment-eviter-les-arnaques
https://www.economie.gouv.fr/cedef/escroquerie-professionnelle