Déjouer l’arnaque au faux relevé d’identité bancaire

31 octobre 2021

Une nouvelle arnaque financière se multiplie depuis quelques mois : le faux relevé d’identité bancaire, à la suite du piratage des boîtes mail.

Vous recevez un mail contenant le RIB d’un artisan, d’une entreprise ou d’un notaire pour le payer par virement. Attention aux tentatives d’escroqueries, par détournement du mail et falsification du RIB. Vous risquez de verser l’argent à un fraudeur.

L’objectif des fraudeurs : se faire verser de l’argent par virement sur leur compte bancaire en détournant la messagerie de leur victime et en modifiant les coordonnées bancaires envoyées.

La technique du faux RIB

Les escrocs détournent tout type de boîtes mails : petites entreprises, collectivités publiques, notaires dans le cadre d’une opération immobilière, et aussi de particuliers. Sans que le piratage de la boîte mail ne soit remarqué.

Les fraudeurs interceptent les mails envoyés ou reçus, avant qu’ils ne soient ouverts et lus par leur destinataire. Sur le mail intercepté, **ils remplacent le RIB mis en pièce jointe et changent l’adresse de l’expéditeur**, et ils renvoient le mail ainsi modifié à son destinataire.

Lorsque le destinataire procède au virement avec le RIB reçu, **les fonds sont transférés sur le compte bancaire de l’escroc**, et non celui de l’entreprise ou du particulier à régler.

Arnaque par email : être vigilant face au risque de piratage

Avant d'effectuer le virement en utilisant le RIB reçu par mail, il est conseillé :

- d'appeler l'artisan, l'entreprise ou le particulier pour vérifier avec lui que le RIB est bien le sien ;
- de vérifier le code pays de la banque figurant sur le RIB : pour une banque française, le code IBAN commence par FR. Un code IBAN commençant par d'autres initiales correspond à une banque étrangère. **Soyez vigilant, les comptes bancaires utilisés par les arnaqueurs sont souvent situés à l'étranger** ;
- de **sécuriser sa boîte mail par une procédure de double vérification** : un mot de passe et l'envoi d'un SMS par exemple. Voir par exemple les bonnes pratiques mise en avant sur le site gouvernemental cybermalveillance.gouv.fr, dispositif national d'assistance et de prévention en sécurité numérique.

Que faire lorsque vous découvrez la tentative de fraude ?

Il existe peu de recours pour récupérer les fonds virés sur le compte bancaire du fraudeur.

En principe, un ordre de virement ne peut pas être annulé dès qu'il a été reçu par la banque. Il est « irrévocable ». Si son exécution est prévue pour une date décalée de quelques jours, l'ordre de virement peut être annulé jusqu'à la fin du jour ouvrable précédant la date prévue pour son exécution.

Mais en cas de fraude, vous devez immédiatement **avertir votre banque de la transaction frauduleuse**. La banque peut mettre en œuvre une procédure de rappel des fonds (« recall ») dans les heures qui suivent l'exécution du virement. Cette procédure est applicable uniquement aux **virements libellés en euros et émis dans la zone SEPA**. La banque de l'émetteur du virement contacte la banque du bénéficiaire, l'accord de ce dernier et de sa banque étant nécessaire pour autoriser le retour des fonds virés. La banque n'a pas l'obligation de procéder à ce remboursement.

En même temps que les démarches auprès de votre banque, vous devez **déposer plainte pour escroquerie** auprès du commissariat de police ou de la gendarmerie proche de chez vous. La copie de votre dépôt de plainte peut vous être demandée par votre banque.

Par « La finance pour tous ». 18 oct.2021