Arnaque - faux conseillers bancaires et faux ordres de virement

La plateforme gouvernementale de sensibilisation aux risques numériques, Cybermalveillance.gouv.fr, voit dans la forte hausse des arnaques au faux conseiller bancaire « le phénomène de 2023 ». Dans son rapport annuel, publié le 5 mars, l'organisme annonce avoir enregistré un bond de 78 % de lecture de son article dédié à cette fraude. « Ils visent absolument tout le monde, via des données récupérées par l'hameçonnage ou en les rachetant », explique Jérôme Notin, directeur général de la plateforme. Cette escroquerie bien rodée ne cesse de monter en puissance et touche désormais aussi bien les professionnels que les particuliers.

Comment ces faux conseillers bancaires opèrent-ils ?

Une personne vous contacte directement par téléphone en se faisant passer pour un conseiller ou un salarié de votre banque ou de son service antifraude. Le numéro de téléphone est celui de votre banque…
Pourtant, il s'agit d'un escroc. Il prétend que vous êtes victime d'opérations frauduleuses et peut, notamment, vous demander :

- de lui communiquer vos identifiants ou coordonnées bancaires et codes reçus par SMS pour qu'elle procède au prétendu blocage de ces opérations ;
- d'effectuer et de confirmer vous-même des actions (ajout d'un bénéficiaire, validation d'une opération bancaire, etc.) directement sur votre espace personnel (via l'application bancaire de votre téléphone ou via votre espace en ligne).

Ce sont ces manœuvres qui permettent à l'escroc d'effectuer des opérations frauduleuses.

C'est une arnaque simple comme un coup de fil, mais la note se chiffre en milliers d'euros

Comment éviter le risque d'arnaque ?

Ne communiquez jamais vos identifiants, codes d'accès et codes confidentiels, dont ceux reçus par SMS, pour valider une opération, et ce, même à une personne prétendant être votre conseiller bancaire appelant depuis le numéro de votre agence et connaissant votre identité (nom, prénom, date de naissance, etc.).

Les escrocs jouent sur la panique : gardez la tête froide et raccrochez dès que des informations confidentielles vous sont demandées. Vous pourrez ensuite contacter vous-même votre banque pour vérification. Et si vous comprenez que vous vous êtes fait arnaquer, alertez le plus vite possible votre banque pour tenter d'effectuer un rappel des virements.

Toutefois, le gros problème, c'est que la banque estime que le client a validé lui-même les paiements. Il est donc difficile de se faire rembourser, d'autant que ce risque n'est pas couvert par les assurances.

Escroquerie au faux ordre de virement : comment s'en prémunir ?

Les escroqueries au faux ordre de virement se multiplient ces derniers temps auprès des entreprises. Sans qu'il s'en aperçoive, un collaborateur peut être amené à virer des fonds sur un compte bancaire frauduleux. Généralement réalisée par téléphone et/ou par mail, cette manœuvre vise toutes les entreprises. Pour y échapper, nous vous proposons d'adopter quelques réflexes.

Comment identifier les risques d'escroquerie au faux ordre de virement ?

Certains signes doivent vous alerter sur un risque d'escroquerie :

- courriels de partenaires commerciaux de l'entreprise avec des adresses électroniques différentes de celles utilisées habituellement ;
- ton insistant de l'interlocuteur au téléphone ;
- caractère urgent du paiement demandé, combiné à l'importance de la somme à payer ;
- demande de modifications de coordonnées bancaires, particulièrement lorsque le nouveau compte bancaire est situé dans un pays autre que celui dans lequel se trouve le bénéficiaire supposé du virement ;
- courriel contenant des fautes d'orthographe, un logo légèrement modifié, un préfixe téléphonique inhabituel, etc.

Quelles mesures préventives adopter si vous devez recevoir une somme d'argent ?

Votre entreprise doit recevoir une somme d'argent :

- indiquez les coordonnées bancaires de paiement de l'entreprise dans les documents contractuels ;
- demandez à votre client de vérifier auprès de vous, personnellement, avant tout paiement, l'authenticité d'un message l'informant d'un changement de coordonnées bancaires.

Quelles mesures préventives adopter si vous êtes le payeur ?

En tant que payeur : vérifiez systématiquement les demandes de changement de coordonnées bancaires de vos fournisseurs.

Pour ce faire, voici les mesures les plus simples à appliquer :

- réalisez un contre-appel avec le numéro de téléphone habituel connu en interne, et non celui fourni par l'escroc ;
- vérifiez sur https://fr.iban.com que la banque associée à l'IBAN bénéficiaire du paiement est bien celle qui est indiquée sur le RIB ;
- interdisez à vos salariés tous paiements sans votre autorisation, y compris en cas d'absence ou d'urgence ;
- vérifiez sur le site Internet de l'interlocuteur s'il signale avoir été victime d'une cyberattaque ;
- sécurisez vos installations informatiques et sensibilisez vos salariés aux dangers d'Internet ;
- si vous le pouvez, évitez les virements bancaires et favorisez d'autres moyens de paiement (chèques, lettres de change…) ;
- limitez la publication d'informations sur vos activités/chantiers (site Internet, réseaux sociaux…) susceptibles de faciliter le travail des escrocs (nom des collaborateurs habilités à réaliser des demandes de virement, liste des fournisseurs, communication sur vos chantiers en cours non encore soldés…) ;
- réalisez une veille régulière des évolutions des escroqueries et de leur fonctionnement.

VOLS ET ARNAQUES mai 24

Un établissement bancaire ne sollicite jamais les informations de connexion de ses clients. Les mots de passe doivent être confidentiels, complexes et régulièrement renouvelés.

Comment réagir si vous êtes victime d'une escroquerie au faux ordre de virement ?

- Contactez immédiatement votre banque pour demander, selon le cas, une suspension du virement en cours ou un rappel des fonds. La rapidité de la réaction est primordiale. Si celle-ci est trop tardive, vous ne pourrez pas obtenir la suspension du virement et vos chances d'obtenir un rappel des fonds seront atténuées ;
- conservez toutes les preuves relatives au virement frauduleux (messages reçus, numéros de téléphone, factures et, plus globalement, tous les éléments pouvant permettre l'identification de la fraude) ;
- bloquez les coordonnées du compte destinataire frauduleux ;
- faites un test antivirus de vos ordinateurs et changez les mots de passe des messageries électroniques ;
- déposez plainte auprès des services de police, en fournissant l'ensemble des éléments de preuve à votre disposition. Vous pouvez également vous connecter à www.cybermalveillance.gouv.fr.

La banque est-elle responsable en cas de virement frauduleux ?

Les établissements bancaires sont tenus à un devoir de vigilance qui leur impose de procéder à des vérifications concernant les opérations effectuées par leurs clients. Ils doivent aussi les mettre en garde contre les irrégularités formelles ou matérielles qu'ils pourraient constater.

Ces irrégularités sont notamment caractérisées lorsque l'opération présente un caractère inhabituel :

- changement soudain des coordonnées bancaires d'un fournisseur ;
- anomalies apparentes du RIB ;
- ordre de virement d'un montant inhabituel ou à destination d'un compte bancaire situé dans un pays inhabituel (exemple : si vous n'avez jamais adressé de virement aux Pays-Bas, la banque devrait s'interroger quant à la normalité de cette opération).

À défaut d'avoir attiré votre attention ou d'avoir sollicité une confirmation de votre part sur un ordre de virement suspect, la responsabilité de votre banque peut être engagée, et des dommages et intérêts peuvent lui être réclamés.

Avant d'envisager un recours à l'encontre de votre banque, l'accompagnement par un professionnel du droit est nécessaire.

Peut-on s'assurer contre la fraude ?

Oui. Des contrats d'assurance permettent de couvrir les conséquences d'une fraude, qu'elle soit externe (comme la fraude au président, par exemple) ou interne (détournement de fonds par un salarié, falsification de chèque…). En fonction du contrat, l'assureur pourra prendre en charge les pertes financières consécutives à la fraude, mais également certains frais induits (recours, honoraires d'experts…).

Certaines mutuelles du bâtiment proposent de telles garanties.

N'hésitez pas à les solliciter.

Le ralentissement sur le marché de l'amélioration-entretien se confirme avec une hausse de l'activité en volume limitée à +1,5 % en glissement annuel au premier trimestre 2024, après +2,6 % le trimestre précédent. Comme craint du fait de la réforme trop brutale de MaPrimeRénov', le tassement ressort encore plus net dans la rénovation énergétique du logement à +0,4 %, après +2,1 % et +3,2 % aux trimestres précédents.