Février 2024

UFC-Que Choisir

L’arnaque au faux conseiller bancaire

L’arnaque au faux conseiller bancaire : une arnaque encore trop fréquente

Une personne vous contacte directement par téléphone, en se faisant passer pour un conseiller bancaire. L’UFC-Que Choisir vous éclaire sur cette arnaque et ses déclinaisons (faux coursier). Retrouvez tous nos conseils.

L'UFC-Que Choisir vous propose de faire un point sur la réglementation et sur vos droits en cas d'arnaque au faux conseiller bancaire et ses différentes déclinaisons.

SOMMAIRE

Qu'est-ce que l'arnaque au faux conseiller bancaire et quelles sont ses déclinaisons ?

L'appel direct d'un faux conseiller bancaire

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 peut même être celui de votre banque. Pourtant, cette personne est un escroc. Elle 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 soi-disant blocage de ces opérations ;
– d'effectuer et de confirmer vous-même des actions (par exemple : 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.

Le phishing suivi de l'appel d'un faux conseiller bancaire

Vous recevez un SMS ou un courriel d'une administration (par exemple la Sécurité sociale) ou d'une société (par exemple la Poste). Il vous est demandé de saisir des données personnelles après avoir cliqué sur un lien.

Après avoir obtenu ces premières informations par phishing, l'escroc vous appelle en se faisant passer pour un conseiller ou un salarié de votre banque. Il prétend que vous êtes victime d'opérations frauduleuses. Il vous met en confiance en vous communiquant des informations précises vous concernant (les informations qu'il a obtenues grâce au courriel ou au SMS frauduleux). Sous couvert de bloquer les opérations frauduleuses, il vous demande de lui transmettre les codes reçus par SMS ou de confirmer des actions directement sur votre application bancaire ou dans votre espace en ligne.

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

L'appel d'un faux conseiller bancaire suivi de l'envoi d'un faux coursier

Désormais, l'arnaque au faux conseiller bancaire ne consiste plus seulement à faire des achats en ligne ou des virements bancaires dont vous n'êtes pas à l'origine. Les fraudeurs vont jusqu'à effectuer des retraits d'espèces après avoir pris possession de votre carte bancaire sous de fausses allégations.

Dans un premier temps, vous êtes contacté par une personne se faisant passer pour un conseiller ou un salarié de votre banque et prétendant que vous êtes victime d'opérations frauduleuses. Elle vous demande de lui communiquer vos identifiants client et/ou vos coordonnées bancaires (dans certains cas, elle a pu obtenir ces informations à la suite d'un phishing). Elle prétend alors, au vu de l'urgence ou de la gravité de la situation, qu'il est nécessaire de mettre en sécurité et/ou détruire votre carte bancaire et vous envoie un coursier à domicile afin de la récupérer.

Les escrocs procèdent ensuite à des retraits à un distributeur automatique de billets (DAB) ou à des paiements en ligne.

© Adobe stock

Le phishing (« hameçonnage ») consiste pour des personnes malveillantes à envoyer des courriels ou sms frauduleux afin d'obtenir des données personnelles ou plus souvent des données bancaires.

© stock.adobe.com

Comment vous en prémunir ?

© Adobe stock

Restez méfiant ! Votre banque ne vous demandera jamais de communiquer des informations confidentielles par téléphone, ni de valider ou bloquer des opérations de paiement à distance. Dans les faits, si une banque veut bloquer une opération, elle n'a pas besoin de votre confirmation et peut le faire seule. De plus, votre banque ne vous enverra jamais de coursier, même en cas d'urgence, pour récupérer vos instruments de paiement.

Attention, les techniques de ces escrocs sont de plus en plus élaborées, telles que :
– des courriels imitant ceux de votre banque ;
– un lien vers une fausse interface ressemblant à votre compte en ligne ;
– un numéro de téléphone affiché correspondant à celui de votre banque ;
– l'emploi du vocabulaire du domaine bancaire ;
– la détention d'informations personnelles vous concernant.

Dans tous les cas, nous vous invitons à raccrocher immédiatement et à ne transmettre aucune information ni cliquer sur un quelconque lien. Ne validez en aucun cas des opérations dont vous n'êtes pas à l'origine, même si votre interlocuteur prétexte qu'il s'agit de les annuler.

Mieux vaut contacter votre conseiller bancaire par vos propres moyens, quitte à attendre l'ouverture de votre agence.

Si un coursier se présente malgré votre refus, ne lui ouvrez pas. Ne lui remettez pas votre carte bancaire, même découpée.

« Une banque ne sollicitera jamais son client pour intervenir et rejeter une opération qu'elle a identifiée comme frauduleuse : elle dispose de tous les moyens nécessaires pour le faire elle-même. »
La Banque de France

© Adobe stock

Lire aussi
Fraudes bancaires – Comment se prémunir, comment réagir ?
Arnaque – Des banquiers très bien imités

Quels recours avez-vous ?

Tout d'abord, signalez sans tarder les opérations dont vous n'êtes pas à l'origine à votre banque. En cas de transmission des coordonnées de votre carte bancaire, faites-y opposition. Modifiez immédiatement le mot de passe de votre espace en ligne. Selon la banque choisie, vous pouvez aussi désactiver les paiements à distance.

Dans le cas où des débits apparaissent, contestez l'opération et demandez le remboursement auprès de votre banque. Elle doit vous rembourser, sauf si elle prouve une négligence grave ou une fraude de votre part.

La transmission des coordonnées bancaires à un tiers, même dans le cas d'une arnaque, a été reconnue par les tribunaux comme une négligence grave. Cependant, plusieurs décisions de justice ont récemment été rendues par des cours d'appel en faveur des victimes de fraude au faux conseiller bancaire. Les juges ont estimé qu'au vu des éléments présentés par les victimes (impression écran des appels, SMS de la banque dans l'historique de conversation, le numéro affiché était celui de la banque, etc.), celles-ci ayant été mises en confiance, la négligence grave des clients n'était pas caractérisée. Vous pouvez tenter d'obtenir le remboursement en vous appuyant sur ces décisions de justice. À ce jour, la Cour de cassation ne s'est pas encore prononcée sur ce type de cas. La jurisprudence est donc encore incertaine et les décisions restent à l'appréciation souveraine des juges.
De plus, dans l'hypothèse où l'opération de paiement a été effectuée sans que la banque ait exigé une **authentification forte**, la banque doit dans tous les cas vous rembourser, à moins de prouver une fraude de votre part. (Pour plus de détails, consultez les pages « Le saviez-vous ? »).

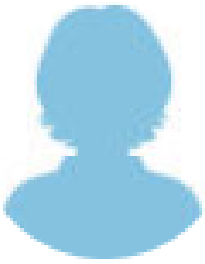
Vous pouvez déposer une préplainte en ligne auprès de la plateforme THÉSÉE sur le site Service-public.fr. Si la fraude porte sur votre carte bancaire, vous pouvez signaler cette pratique sur le téléservice Perceval.


© Adobe stock

Lire aussi
Fraude bancaire - BNP Paribas condamné à rembourser un client
Fraudes bancaires - Les banques de nouveau rappelées à l'ordre

Articles L.133-18, L.133-19, L.133-23 et L.133-44 du Code monétaire et financier ; cour d'appel de Versailles 28/03/2023 n° 2107299 ; cour d'appel de Douai 05/01/2023 n° 21/04625 ; cour d'appel de Poitiers 12/09/2023 n° 22/00055 ; Cour de cassation, chambre commerciale 30/08/2023 n° 22-11707

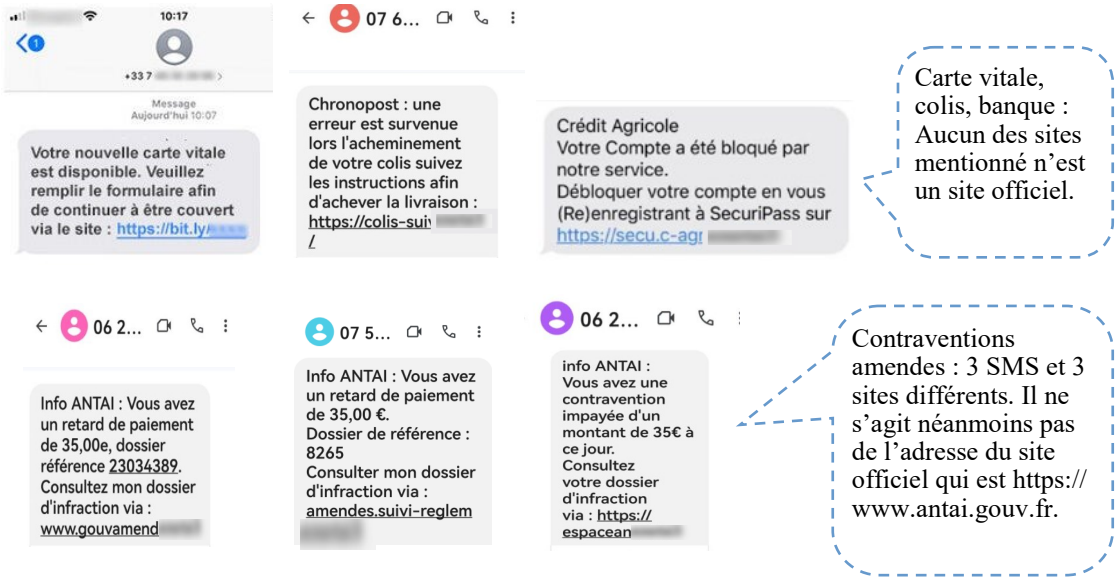
Témoignage Claire D., victime de l'arnaque au faux conseiller bancaire.



« J'ai reçu un courriel me demandant de payer une amende routière. Je ne me suis pas méfiée puisque je m'attendais à recevoir une amende pour stationnement impayé. J'ai donc cliqué sur le lien et donné mes coordonnées bancaires pour la payer. Quelque temps après, un conseiller de ma banque disant que des retraits suspects étaient en cours sur ma carte m'a contactée. Je devais partir le lendemain en vacances, j'étais paniquée. Il m'a rassurée en me disant qu'il allait tout bloquer et m'a indiqué qu'il envoyait un coursier sécurisé pour récupérer ma carte bancaire et en rééditer une en urgence. Il connaissait ma date de naissance, celle de mon mari, le numéro de ma carte bancaire. Il appelait avec le numéro de téléphone de notre agence bancaire. Mise en confiance et n'ayant jamais donné mon code confidentiel, je pensais que ça ne craignait rien. Or, il a réussi à modifier mon plafond de retrait sur mon espace en ligne et a ensuite retiré plus de 3 000 € en espèces. Aujourd'hui, je bataille encore avec ma banque pour être remboursée. »

Quelques exemples de SMS douteux

Ces messages sont là pour recueillir vos coordonnées bancaires ou personnelles. Ne répondez pas, ne cliquez pas sur le lien !



- Ces SMS sont émis par des numéros de téléphone portable et non par des numéros courts officiels.
- Le lien mentionné est différent de celui du site officiel.
- Ces SMS concernent des problématiques courantes de notre vie quotidienne : réception d'un colis, paiement d'une amende, renouvellement d'une carte vitale, gestion des comptes bancaires… C'est cela qui crée souvent le doute et vous incite à cliquer sur le lien.

⇒ Pensez à vérifier l'adresse officielle.
⇒ Connectez-vous directement à votre compte client ou à l'application concernée.
⇒ Contactez le service client ou votre conseiller directement.

Le saviez-vous ?

Qu'est-ce que l'authentification forte ?

© Stock Adobe

L'authentification forte (ou double authentification) est un dispositif permettant de vérifier votre identité pour plus de sécurité. Il faut au moins 2 des 3 éléments suivants :
– un élément de connaissance (mot de passe, code secret ou question secrète) ;
– un élément de possession (téléphone mobile ou clé USB) ;
– un élément biométrique (empreinte digitale, forme de l'iris ou reconnaissance vocale).

Elle doit s'appliquer dès lors que le montant de l'opération dépasse 30 € et que le montant cumulé des précédentes opérations depuis la dernière authentification forte du client dépasse 100 € ou que le nombre des précédentes opérations de paiement depuis la dernière authentification forte du client dépasse 5 opérations de paiement électronique à distance individuelles consécutives.

Vous pouvez consulter notre article « Paiements en ligne : la double authentification s'impose ».

Refus de remboursement des fraudes bancaires : la plainte déposée par l'UFC-Que Choisir est toujours en cours

L'UFC-Que Choisir, face aux nombreux refus de remboursement injustifiés des banques, a déposé plainte contre 12 établissements pour pratiques commerciales trompeuses le 28 juin 2022. La plainte contre la banque Nickel a été classée sans suite mais pour les autres banques, l'enquête est toujours en cours. L'UFC-Que Choisir, à travers la multitude de refus injustifiés, a mis au jour une véritable stratégie des banques pour s'affranchir de leur obligation de démontrer la négligence personnelle de leurs clients afin de refuser de les rembourser (voir notre article « Refus de remboursement des fraudes bancaires : l'UFC-Que Choisir dépose plainte contre 12 banques »).

Vous trouverez également à votre disposition deux lettres types :
Fraude à la carte bancaire – Contestation de l'utilisation d'un code 3D Secure
Fraude à la carte bancaire – Demande de remboursement

Le saviez-vous ?

Les pénalités prévues en cas de retard de remboursement des opérations non autorisées

© Stock Adobe

Par principe, dès lors qu'une opération non autorisée est signalée à la banque, cette dernière est tenue de procéder immédiatement au remboursement de ladite opération au plus tard à la fin du premier jour ouvrable suivant. Cette règle comporte une exception si la banque a de bonnes raisons de soupçonner une fraude de l'utilisateur du service de paiement et si elle communique ces raisons par écrit à la Banque de France.

Depuis le 19 août 2022, des pénalités sont prévues en cas de retard dans le remboursement :

« 1° Les sommes dues produisent intérêt au taux légal majoré de 5 points ;
« 2° Au-delà de 7 jours de retard, les sommes dues produisent intérêt au taux légal majoré de 10 points ;
« 3° Au-delà de 30 jours de retard, les sommes dues produisent intérêt au taux légal majoré de 15 points. »

Article L.133-18 du Code monétaire et financier modifié par l'article 22 de la loi n° 2022-1158 du 16 août 2022

Et si votre banque vous demande de déposer plainte ?

L'UFC-Que Choisir constate que les banques conditionnent souvent le remboursement à un dépôt de plainte préalable. Or les services de police et de gendarmerie sont débordés par ces dépôts de plainte et refusent parfois de prendre la plainte des victimes de fraudes bancaires. En tout état de cause, la banque ne peut exiger un dépôt de plainte pour traiter votre demande de remboursement. Cette formalité n'est pas imposée par la réglementation.

Si vous souhaitez déposer plainte, vous pouvez le faire par écrit en portant plainte contre X. En revanche, faute de certitude sur les moyens employés par les fraudeurs, évitez d'évoquer des hypothèses. Restez factuel en indiquant uniquement le(s) débit(s) frauduleux constatés. En effet, la banque peut chercher des éléments dans votre déclaration pour considérer que vous avez été négligent dans la conservation de vos données bancaires et refuser de vous rembourser. Néanmoins, la négligence grave ne se présume pas. Elle devra être prouvée par la banque.

Retrouvez toutes les informations utiles sur le site de votre association locale UFC-Que Choisir.

66% de votre don est déductible de vos impôts dans la limite de 20% de vos revenus imposables.

© Adobe Stock

L'UFC-Que Choisir est à vos côtés pour vous renseigner et vous orienter dans vos démarches.

Un litige ?

L'UFC-Que Choisir est aux côtés des consommateurs pour les aider à résoudre leurs litiges avec les professionnels. Nos adhérents peuvent bénéficier d'un accompagnement personnalisé dans le but d'obtenir une résolution amiable de ce différend.

Si vous souhaitez obtenir une assistance ou une intervention de notre part, cela nécessite de s'acquitter au préalable d'une cotisation annuelle auprès de l'UFC-Que Choisir. En effet, en tant qu'association de défense des consommateurs, nous ne pouvons délivrer de consultations juridiques qu'à nos membres.

Devenir adhérent de l'UFC-Que Choisir, c'est rejoindre un mouvement et bénéficier de tous les avantages liés à l'adhésion :

– Un appui et une promotion de vos actions individuelles.

– Une information sur vos droits.

– Une participation à la défense des consommateurs.

Ce que nous ne pouvons pas faire :

– Missionner un expert, un auxiliaire de justice comme un avocat ou un huissier.

– Vous assister ou vous représenter devant une juridiction ou tout organe ayant compétence pour trancher votre litige.

– Intervenir dans des matières ne relevant pas de notre objet statutaire comme le droit de la famille, le droit du travail, le droit fiscal.

Contactez-nous !

Votre Association locale
UFC-Que Choisir

Pour que notre association puisse vous accompagner dans le traitement de votre litige, il est nécessaire (loi n°71-1130 du 31 décembre 1971) que vous en deveniez adhérent. L'adhésion est distincte de l'abonnement à nos publications : elle permet aux associations UFC-Que Choisir de défendre l'intérêt individuel et collectif des consommateurs.