



Comment j'ai failli me faire arnaquer

(Enregistré le 26 juin 2026)

Introduction

Lucile Rives : Il y a quelque temps, je dinais avec des amies. Mon amie Andrea nous a raconté qu'elle venait d'être victime d'une arnaque au faux conseiller bancaire.

Andrea : Je me suis vraiment faite escroquer. Le faux conseiller bancaire a réussi à me faire sortir de chez moi, très vite et à vélo. Je dois avouer, en toute humilité, que l'arnaque était très bien conçue.

Lucile Rives : Nous étions huit autour de la table. Certaines connaissaient des victimes d'arnaques spectaculaires : arnaque aux faux diamants, arnaque à la romance. Et trois d'entre nous avions été les cibles ou les victimes directes d'arnaques au faux conseiller bancaire. Y compris Andrea et moi !

Andrea est avocate et elle pensait qu'elle n'avait pas l'âge de se faire arnaquer. Pour ma part, je sortais de l'enregistrement d'un épisode de podcast dans lequel Marguerite Collignan, directrice de l'Éducation financière de la Banque de France, nous avait expliqué ceci :

Marguerite Collignan : Les escrocs, pour aller jusqu'au bout de leurs arnaques, jouent sur les peurs. Dans le cas des jeunes, ils jouent sur la conviction que l'on peut devenir riche sans risque. Pour les seniors, ils jouent sur les sentiments d'urgence, sur les émotions trop fortes. Mais si on prend le milieu de la population, on peut aussi être victime de fraude.

Lucile Rives : Les arnaques sont donc des processus extrêmement bien conçus. Même si vous pensez être informés, vous pouvez être piégés. Je vous partage donc nos mésaventures, en espérant que vous ne croiserez jamais la route d'un faux livreur, d'un faux conseiller bancaire, d'un faux Brad Pitt ou d'un faux vendeur de diamants. Mais si cela devait vous arriver, j'espère que le souvenir de cet épisode allumera dans votre esprit une petite lumière de vigilance qui vous protégera.

Je m'appelle Lucile et je travaille à la Banque de France. Bienvenue dans l'Eco en court.

Les faits

Lucile Rives : J'attendais un colis. Je m'étais organisée pour le réceptionner mais comme il n'arrivait pas, j'ai dû m'absenter un court moment : faire quelques courses, récupérer les enfants à l'école... À peine rentrée, j'ai reçu ce message :

Livreur : Bonjour c'est le livreur. Je suis venu il y a 30 minutes pour vous déposer un colis. Malheureusement il n'entrait pas dans la boîte aux lettres. Du coup, je vous ai envoyé un SMS pour reprogrammer la livraison.

Lucile Rives : J'étais contrariée d'avoir manqué cette livraison. Alors, tout en rangeant les courses et tout en aidant aux devoirs, j'ai cliqué sur le lien qui accompagnait le message vocal pour reprogrammer la livraison.

Est-ce que j'ai trouvé étrange qu'il faille payer 47 centimes pour être à nouveau livrée ? Oui et non. Oui parce que c'était la première fois qu'on me facturait ce service, et non parce qu'après tout c'était normal, dès lors qu'un livreur allait devoir se déplacer de nouveau pour effectuer la livraison. J'ai donc donné toutes les informations qui m'étaient demandées : identité, adresse, et bien-sûr carte bancaire.

C'est quand j'ai reçu le même message, quelques jours plus tard, alors que j'avais enfin reçu le fameux colis, que j'ai suspecté quelque chose de curieux. Dans le doute, j'ai fait opposition sur ma carte bancaire et j'ai cessé d'y penser. Mais les escrocs, eux, n'en avaient pas terminé avec moi.

Lucile Rives : Une semaine plus tard, j'ai reçu un appel. Un homme, calme et concerné, se présente comme en charge de la lutte contre la fraude au sein de la banque où je suis cliente. Il me rassure et m'alerte à la fois : ma carte bancaire a bien été mise en opposition mais un peu trop tard. Un prélèvement de 600 euros vers Abidjan est en attente. Mon amie Andrea a reçu le même genre de coup de fil : ce sont 500 euros à destination de l'Algérie qui doivent lui être prélevés.

J'ai raconté nos mésaventures à Pierre Bienvenu, responsable du Service des moyens de paiement à la Banque de France.

Pierre Bienvenu : La fraude concerne réellement tout le monde, y compris les personnes averties sur ce type de problèmes. On a parfois l'image des fraudeurs qui viendraient toucher particulièrement les personnes âgées. En réalité, les chiffres du ministère de l'Intérieur montrent que les premières victimes d'escroquerie financière sont les 25-49 ans, c'est-à-dire la population active. Et en même temps, les fraudes concernent toutes les classes d'âge, toutes les catégories socio-professionnelles. Mais effectivement surtout la classe des 25-49 ans, qui ont du patrimoine et qui ont peut-être un agenda très chargé, dans lequel s'engouffrent les fraudeurs. A l'instar de ton profil, Lucile. Tu es donc complètement dans la cible.

Lucile Rives : Nos faux chargés de lutte contre la fraude, outre le fait qu'ils veulent nous escroquer, ont aussi en commun de vouloir nous aider. Aussi, le faux conseiller de mon amie

Andrea prend-il les devants. Par mesure de précaution, il lui dit : « On bloque la carte, mais ne vous inquiétez pas, vous pouvez toujours payer avec votre téléphone. On va bloquer la carte uniquement en ligne ».

Andrea : Je suis alors très rassurée : ces procédures sont décidément bien réalisées, la carte est bloquée en ligne seulement.

Pierre Bienvenu : Les fraudeurs se présentent comme des personnes de confiance, qui vont vous aider dans ce quotidien chargé. À ce moment-là, les gens apprécient ; les victimes apprécient ce sentiment d'être épaulé, aidé. Donc cela diminue un peu le niveau de vigilance.

Lucile Rives : Effectivement, nos faux chargés de lutte contre la fraude doivent gagner notre confiance car, pour nous escroquer, ils ont besoin de nous : nous devons leur transmettre un code. Pour ce faire, ils nous enjoignent de nous rendre en urgence dans une agence bancaire. Je trouve la démarche étrange et dans un éclair de lucidité, je décide de raccrocher et d'appeler mon vrai conseiller bancaire. Il me confirme que ma carte bancaire est en opposition, qu'aucun prélèvement suspect n'est en attente et finalement, qu'aucune opération frauduleuse ne s'est présentée sur mon compte.

Pierre Bienvenu : Les actions techniques en matière de contrôle à la fraude fonctionnent : tu as certes transmis ton numéro de carte bancaire - et désormais celui-ci est mis en opposition - mais les fraudeurs n'ont pas réussi, avec ton seul numéro de carte bancaire, à réaliser la moindre opération. Car aujourd'hui, en tout cas pour payer sur Internet, cette authentification forte est nécessaire. Donc les fraudeurs avaient besoin de toi pour une action supplémentaire : confirmer la transaction. C'est la raison pour laquelle le seul fait de donner son numéro de carte bancaire, même si c'est effectivement une négligence, ne suffit plus, ou en tout cas pas toujours, pour réaliser une opération de paiement. Ce qui est une bonne nouvelle.

Lucile Rives : Mon amie Andrea, elle, n'a malheureusement pas eu le réflexe de raccrocher. Alors, avec le soutien indéfectible de son faux conseiller et vrai escroc, elle s'est mise en quête de l'agence bancaire la plus proche pour lui communiquer un code d'authentification forte.

Andrea : Il m'a dit « On va faire une opération ensemble pour éviter le retrait sur votre compte. Vous devez aller dans votre agence, pour confirmer que vous êtes bien en France et que ce n'est pas vous qui effectuez le retrait en Algérie. Quand pouvez-vous y aller ? »

Lucile Rives : Elle se rend dans une première agence où les distributeurs ne marchent pas.

Il la rappelle lorsqu'elle est devant le distributeur, qui ne fonctionne pas.

Andrea : Je lui demande : « Comment fait-on ? » Je sens que nous sommes partenaires, que nous cherchons une solution ensemble.

Lucile Rives : Le piège s'est refermé. Elle se rend dans une deuxième agence.

Andrea : Je fonce vers l'arnaque ! Mais l'agence est fermée.

Lucile Rives : L'urgence à agir, le sentiment de faire équipe, l'escroc n'a même plus besoin de lui demander d'essayer de se rendre dans une troisième agence. Elle le décide d'elle-même.

Andrea : Il m'a dit : « Maintenant, voici ce que vous devez faire, pour obtenir un code de retrait à distance par SMS. »

Pierre Bienvenu : Ce sont des organisations criminelles qui collectent les informations sur tous les parcours bancaires, toutes les procédures de sécurité des établissements bancaires et qui sont par conséquent en mesure d'accompagner le client en fonction de la banque dans laquelle il est client. Ils sont très stratèges, car non seulement ils utilisent un vocabulaire de l'empathie, de l'accompagnement, pour rassurer le client, mais également ils connaissent exactement chaque étape du parcours sur l'application bancaire, ce qui rassure immédiatement le client.

Andrea : Il me dit : « C'est l'étape finale, il faut autoriser le retrait, mais rien ne sera retiré, il n'y a pas de problème ». Et là, je commence à rire. Je lui réponds : Comment puis-je savoir que vous n'êtes pas un arnaqueur ? Prouvez-moi que vous n'êtes pas un arnaqueur... Franchement, je ne vais pas me faire arnaquer. On m'en parlera quand j'aurai 80 ans. Alors, le code, pas de problème, merci pour votre assistance.

Lucile Rives : Le record de vitesse de la traversée de Paris à vélo et 500 euros de moins plus tard, Andrea se demande encore comment tout cela a bien pu lui arriver.

Qui prend en charge les frais ?

Lucile Rives : Outre le sentiment très désagréable de s'être fait escroquer ou d'avoir failli se faire arnaquer, notre négligence à un prix.

Pierre Bienvenu : C'est le sujet sensible des frais. Voici le principe général dans les fraudes aux moyens de paiement : sauf négligence grave de la part du client - et toute la question est de savoir si une négligence grave a été commise - la banque doit rembourser les opérations de paiement frauduleuse que le client a subies. S'il y avait des opérations débitées sans authentification forte de ta part, elles auraient été automatiquement remboursées. S'il y a une authentification forte de ta part, alors il est demandé aux banques d'analyser le contexte de l'opération, et la façon dont l'authentification forte a été réalisée. À ce moment, le traitement sera au cas par cas, mais la banque doit décider si une négligence grave a été commise effectivement ou pas. Si elle juge qu'une négligence grave de ta part a eu lieu, elle ne te remboursera pas, mais tu peux évidemment poursuivre le dialogue ou le débat avec ta banque en saisissant le service de réclamation, puis éventuellement le médiateur, et en toute fin de processus, l'action en justice qui peut être aussi un recours pour obtenir gain de cause et trancher sur la présence ou non d'une négligence grave.

Que peut-on faire pour prévenir la fraude ou à défaut, limiter les problèmes ?

Lucile Rives : Tout d'abord, il faut adopter une posture de vigilance et se rappeler que nos données sont précieuses : ne communiquons pas nos codes d'authentification forte et transmettons nos numéros de carte bancaire uniquement sur des sites de confiance.

Par ailleurs, une banque n'a pas besoin de nous pour bloquer une opération : si elle estime qu'une transaction est trop risquée, elle peut décider de ne pas l'exécuter. Et elle ne nous demandera jamais de lui communiquer nos codes. Il est en outre très peu probable que nos conseillers bancaires nous appellent à partir d'un numéro de téléphone qui commence par 06 ou 07.

Rappelons-nous également qu'il n'y a pas d'urgence : nous pouvons toujours prendre le temps de vérifier l'identité de nos interlocuteurs ou des bénéficiaires de nos virements. Dans le doute, n'hésitons pas à appeler nos contreparties ou notre conseiller bancaire.

Il est aussi possible de signaler les SMS frauduleux au 33700. Ce numéro est géré par les opérateurs téléphoniques : à partir des signalements, ils peuvent enquêter pour vérifier si l'activité de la ligne est cohérente avec les conditions générales d'utilisation de leurs services et le cas échéant, la couper.

Enfin, si vous pensez avoir été victime d'une fraude à la carte bancaire, faites rapidement opposition.

Pierre Bienvenu : Tu as effectivement bien fait de faire opposition sur ta carte, car cela signifie que tu repars de zéro et que l'on est certain désormais que ton numéro de carte, qui se trouve quelque part sur le darknet, ne pourra jamais être utilisé pour réaliser une opération de paiement.

Jusqu'où s'inquiéter ?

Lucile Rives : Arnaques redoutablement rodées, informations négligées qui peuvent être vendues sur le darknet, profils de cibles et de victimes variés... jusqu'où doit-on s'inquiéter ?

Pierre Bienvenu : Le sujet est certes préoccupant mais si nous revenons aux chiffres, notamment concernant la fraude à la carte bancaire, nous observons plutôt une tendance baissière depuis plusieurs années, qui se poursuit. La sécurité des paiements par carte a été profondément renforcée, à la fois par l'authentification forte et par toutes les actions mises en place par l'écosystème des paiements, qui utilise aussi les outils d'intelligence artificielle pour vérifier la cohérence des transactions.

Lucile Rives : Dans tous les cas, restons vigilants. Merci à toutes et tous de nous avoir écoutés. Un merci tout particulier à Pierre Bienvenu et Andrea pour leur contribution à cet épisode. S'il cet épisode vous a plu, n'hésitez pas à le partager, à nous laisser des commentaires et des étoiles. À bientôt !