Côte-d'Or

Arnaque au compte bancaire : des

Le *spoofing*, c'est cette arnaque qui voit des escrocs s'introduire dans votre ordinateur pour tenter de s'octroyer des virements bancaires frauduleux. Dans notre département, les victimes sont de plus en plus nombreuses. Et elles ont parfois du mal à faire face.

Elle se sent « abandonnée ». La Dijonnaise Françoise L. fait partie des nombreux Côte-d'Oriens victimes ces derniers mois de *spoofing*, ces arnaques qui conjuguent fausses promesses au téléphone et piratage informatique pour vider les comptes bancaires des clients malheureux.

> « J'ai même tenté ma chance chez Julien Courbet ! »
> **Françoise L.**

L'histoire de Françoise commence en avril 2022. « J'avais l'habitude de vérifier mes comptes tous les matins », raconte-t-elle. « Un jour d'avril, sans explication, il n'était plus possible de me connecter. J'avais la mention "réessayez dans une heure", "réessayez dans deux heures", "réessayez demain matin"… Malgré de multiples appels à mon conseiller, à la Caisse d'épargne, je n'avais pas de réponse. Le 18 mai, j'ai fini par demander une capture d'écran de mon compte, facturée d'ailleurs par la Caisse d'épargne, et j'ai alors pu constater que, le 5 mai, cinq virements avaient été effectués de mon compte sur une appli d'échange de devises et de services bancaires, ce que je n'avais évidemment pas validé. » Un scénario battu en brèche par la Caisse d'épargne *(lire par ailleurs)*.

Deux plaintes successives

Le 7 mai, selon Françoise, trois autres virements ont été effectués pour un montant total de 6 500 €. « En vérifiant mes comptes sur la capture d'écran, j'ai compris aussi que 3 000 € avaient été prélevés le 19 avril et restitués le 26 avril, sans explications ni alerte de ma banque. Je me suis rendue à mon agence habituelle, et le conseiller m'a répondu que je n'avais… qu'à changer de banque. J'ai donc joint la Maison de la justice et du droit de Chenôve pour être conseillée, puis j'ai déposé plainte à la gendarmerie. Mais malgré la demande de conciliation de la Maison de la justice et du droit, je n'ai obtenu aucun remboursement. J'ai même contacté l'appli d'échange de devises et de services bancaires, qui m'a confirmé que c'était à la Caisse d'épargne de venir vers elle. »

Un mystérieux M. Ossona ajouté aux bénéficiaires

Le cauchemar s'accélère encore le 28 novembre : « J'ai reçu trois SMS de la Caisse d'épargne en un quart d'heure, m'indiquant qu'un bénéficiaire nommé "Ossona" venait d'être ajouté pour un virement de 2 500 €. J'ai tout bloqué, je me suis de nouveau rendue à mon agence… et j'ai appris que mon livret A avait été vidé la veille, toujours sans alerte de ma banque. J'ai donc aussi porté plainte au commissariat et je me suis rapprochée de l'UFC-Que choisir. J'ai même tenté ma chance chez Julien Courbet ! Au total, ce sont donc 9 500 € qui m'ont été débités frauduleusement, depuis maintenant plus d'un an. Avec ma petite retraite d'artisan d'à peine 900 €, je dois faire attention à chaque dépense. Heureusement, j'ai pu compter sur l'aide de quelques amis. Mais quand on est client de la même banque depuis cinquante ans, être traitée de la sorte est incompréhensible. »

● **Dossier réalisé par Frédéric Joly**
frederic.joly@lebienpublic.fr

> « Avec ma petite retraite d'artisan d'à peine 900 €, je dois faire attention à chaque dépense. Heureusement, j'ai pu compter sur l'aide de quelques amis. Mais quand on est client de la même banque depuis cinquante ans, être traitée de la sorte est incompréhensible. »
> **Françoise L.**

9 500

C'est, en euros, la somme totale qui aurait été débitée frauduleusement, depuis maintenant plus d'un an, sur le compte de Françoise.

La Caisse d'épargne se défend

Contactée, la Caisse d'épargne Bourgogne-Franche-Comté répond assez sèchement à la version de Françoise L. « Les mouvements auxquels vous faites référence ont été validés *via* le système d'authentification forte qui oblige la personne à valider l'opération sur son téléphone, d'où notre refus de rembourser ces sommes », indique-t-elle d'emblée. « Par ailleurs, la cliente a saisi la médiation de la Fédération bancaire française, et son dossier est donc en attente de l'avis du médiateur. Cette cliente a aussi été sensibilisée de nombreuses fois par nos conseillers sur les risques d'escroqueries, différentes mesures ont été mises en place à différents moments pour l'aider. Plus globalement, nous sensibilisons très régulièrement notre clientèle par le biais de messages sur notre application bancaire et notre site internet sur le fait de ne jamais donner ses codes bancaires ni valider des opérations que l'on n'a pas entreprises soi-même. Nous insistons sur un point capital : à partir du moment où une personne communique à un tiers ses codes bancaires (ce que ne demande jamais l'établissement bancaire) ou valide, *via* notre système d'authentification forte, des opérations qu'elle n'a pas initiées, la banque, quelle qu'elle soit, ne peut plus agir, d'autant plus quand les fonds partent vers l'étranger. Nos conseillers commerciaux sensibilisent régulièrement leurs clients, et comprennent leur détresse lorsqu'ils se rendent compte qu'ils ont été victimes d'une escroquerie. Des alertes constantes sont présentes sur l'espace banque à distance des clients. Des campagnes radiophoniques ont été mises en place par la Fédération bancaire française (FBF) afin de mettre en garde les consommateurs sur ce sujet. Il appartient alors à la justice d'agir contre les escrocs. »

▶ Sur le Web

Avez-vous déjà été victime de *spoofing* (arnaque téléphonique au compte bancaire) ?

17 % Souvent

67 % Jamais

16 % Je ne sais pas de quoi il s'agit

Total des votes : 2 641

CDO02 - V1

victimes nombreuses et démunies

L'arnaque du *spoofing* passe souvent par une discussion téléphonique de « mise en confiance ». Photo d'illustration Emma Buoncristiani

La gendarmerie monte en gamme sur le numérique

Afin de lutter contre le *spoofing*, l'adjudant Fabrice Courbez, référent cyber pour le Groupement de gendarmerie de Bourgogne-Franche-Comté, a plusieurs cordes à son arc numérique.

« Je mise notamment beaucoup sur la prévention *via* les différentes mairies », détaille-t-il. « Grâce à un envoi de *mails* à leurs administrés, nous pouvons détailler ce qu'est le *spoofing*, les techniques utilisées par les escrocs, et les meilleurs moyens de s'en protéger. Nous utilisons aussi les réseaux sociaux pour diffuser ces messages d'explication et de prévention. Pour ce type d'arnaque, on se rend souvent compte que le premier risque, c'est le facteur humain, comme ouvrir une pièce jointe qui va permettre à l'escroc d'infiltrer un système informatique et récupérer des données personnelles, bancaires par exemple. »

Si 40 % des entreprises, à l'échelle française, ont désormais investi dans la cybersécurité, c'est moins évident pour des particuliers qui sont attaqués de façon plus sporadique, mais non moins féroce.

L'adjudant Fabrice Courbez est le gendarme référent cyber pour le groupement de gendarmerie de Bourgogne-Franche-Comté. Photo E. Bu.

La brigade la plus proche ou Pharos

« Le plus efficace, dès qu'on est victime, c'est d'aller voir la brigade de gendarmerie la plus proche ou de signaler les faits sur Pharos, notre plateforme qui traite des cyberharcèlements », conseille l'adjudant Courbez. « Depuis février 2018, un gendarme est également joignable sept jours sur sept et vingt-quatre heures sur vingt-quatre pour tout ce qui concerne le numérique. »

« Tout le monde peut être touché »

L'adjudant Courbez poursuit : « Enfin, COMCyberGEND, ou commandement de la gendarmerie dans le cyberespace, a été lancé en 2021 pour animer, coordonner et renforcer les capacités de la gendarmerie dans le domaine numérique, qu'il s'agisse de prévention, de formation ou d'investigations. Tout le monde peut être touché. On pense souvent que les personnes âgées sont les seules cibles possibles, mais nous avons aussi des jeunes qui se font avoir par les envois en masse des escrocs. »

« Les textes protègent les clients », rappelle la police

Il l'avoue lui-même : son petit bureau ne désemplit pas de plaignants qui se sont fait arnaquer sur le web, et la pile de plaintes à traiter dans ce domaine grandit jour après jour. Au commissariat de Dijon, le brigadier-chef Éric Lemoine est le référent financier de la sûreté départementale. Il en convient également : les techniques des escrocs sont de plus en plus évoluées. « Aujourd'hui, il est devenu très facile de pirater le numéro de téléphone de votre conseiller bancaire pour vous faire croire que c'est lui qui vous appelle », détaille-t-il. « Sauf que même si son numéro s'affiche sur votre téléphone, un banquier qui vous appelle à 22 heures ou pendant un jour férié, c'est impossible ! »

« Dès qu'on a un doute, raccrocher »

« La première chose à faire quand on a un doute, c'est donc tout simplement de raccrocher et de vérifier auprès de sa banque, même s'il faut attendre le lendemain et passer une nuit difficile », ajoute-t-il. Deuxième règle : ne jamais donner à quelqu'un qui se réclame de votre banque au téléphone les codes d'accès à vos comptes. « Un escroc peut pirater votre système informatique, récupérer vos données personnelles et donc avoir accès à vos comptes, mais s'il veut faire un virement frauduleux, il lui faudra vos codes de confirmation », rappelle Éric Lemoine. « Autre astuce : se fixer des plafonds de dépenses relativement bas, quitte à les relever en cas de dépense exceptionnelle, car les escrocs auront toujours tendance à dépenser le plus possible sur votre compte. Leur localisation par téléphone est souvent difficile ; car ils utilisent des cartes prépayées. Les virements frauduleux partent souvent de l'étranger, ce qui rend beaucoup plus difficiles les enquêtes de police et les démarches judiciaires. »

Le commissariat de Dijon traite régulièrement des plaintes pour *spoofing*. Photo E. Bu.

Les banques face à leurs responsabilités

Éric Lemoine sait aussi que l'autre défi des clients piratés, c'est de se faire rembourser : « Les banques ont fait des efforts en multipliant, notamment, les messages de prévention. Mais elles ont encore tendance à traîner des pieds pour rembourser des clients de bonne foi. Mais les textes protègent les clients : dans plusieurs arrêts publiés ces dernières années, la Cour de cassation, c'est-à-dire la plus haute juridiction, a confirmé plusieurs principes. Le premier : les clients ne sont pas responsables, *a priori,* du piratage de leur compte bancaire, quand bien même les paiements ont donné lieu à une authentification forte. Le deuxième : la banque a un devoir de vigilance et doit prévenir son client en cas d'activité inhabituelle sur son compte. Le troisième : c'est à la banque qu'incombe la charge de la preuve, c'est-à-dire que ce n'est pas au client de démontrer qu'il a pris toutes les mesures raisonnables pour préserver la sécurité de ces données de sécurité, mais à la banque de prouver qu'il a été négligent. » Et c'est rarement évident, en l'absence d'aveux de la victime.