Piratage bancaire
Des clients mis à terre

Enquête

Les escrocs s'introduisent sur l'espace bancaire des clients et parviennent à vider leurs comptes par virements frauduleux. Les banques refusent de rembourser, invoquant la négligence et laissent les clients dans le désarroi.

Nous en avons assez de passer notre temps à enregistrer les dépositions de victimes de fraudes. Donc, voici l'article de loi qui oblige votre banque à rembourser… » C'est un officier de police de Besançon excédé qu'Yves a devant lui. Ce septuagénaire est venu déposer plainte après avoir constaté un virement frauduleux de 1 400 €.

Depuis plusieurs mois, ce type de piratage se multiplie, au point d'être devenu le sujet de plainte n° 1 des clients dans le secteur bancaire. Le fraudeur s'introduit sur l'espace personnel du titulaire, parvient à effectuer des virements sur un ou plusieurs comptes parfois situés à l'étranger.

Points communs à toutes les victimes : les sommes détournées sont considérables, et elles ne sont pas remboursées par leur banque, qui les accuse au contraire de négligence.

LE PIÈGE SE REFERME… ET LE COMPTE EST VIDÉ

Cette escroquerie, maintes fois rapportée à «60» par des victimes depuis un an, implique très souvent une usurpation d'identité. Fin mars, Sandra a ainsi reçu l'appel d'un homme se présentant comme employé du service de lutte contre la fraude de sa banque. « *Il détient mon nom, mon numéro de portable, de compte et le nom de mon conseiller, je n'ai aucune raison de me méfier. Il m'annonce qu'on est en train de vider mon compte, il me demande de faire immédiatement des manipulations pour tout stopper* ». En quelques secondes, le piège est refermé : « *Il a vidé mon compte de 4 295 €, soit toutes nos économies.* » Sandra alerte son conseiller dès qu'elle découvre les dégâts, qui lui promet un remboursement. Le lendemain, le discours a complètement changé. « *Le conseiller m'accuse de négligence, il ne veut plus me rembourser mais me propose un crédit pour m'en sortir…* »

Des clients persuadés d'être appelés par leur conseiller…

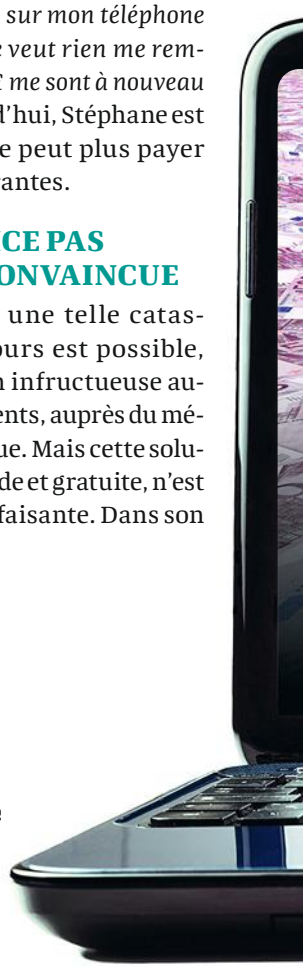
Stéphane s'est également fait voler 4 500 € après un piratage et un virement frauduleux. Sa banque promet un remboursement, après son dépôt de plainte. Une semaine après, elle lui restitue les sommes envolées. « *Puis elle me contacte en me disant que ce n'est pas leur faute, un pirate s'est installé sur mon téléphone et, du coup, elle ne veut rien me rembourser, les 4 500 € me sont à nouveau prélevés !* » Aujourd'hui, Stéphane est à découvert, et ne peut plus payer ses dépenses courantes.

LA MÉDIATRICE PAS VRAIMENT CONVAINCUE

Que faire face à une telle catastrophe ? Un recours est possible, après réclamation infructueuse auprès du service clients, auprès du médiateur de la banque. Mais cette solution, si elle est rapide et gratuite, n'est pas toujours satisfaisante. Dans son

NOS CONSEILS POUR LIMITER LES RISQUES

- Ne vous connectez jamais à partir d'un lien commercial ou bancaire envoyé par mail.
- Ne fournissez jamais d'informations par téléphone : plus c'est urgent, plus c'est suspect.
- Ne répondez jamais à un courriel commercial, n'ouvrez pas la pièce jointe. En cas de doute, connectez-vous au site en question ou contactez votre banque.
- Gardez l'antivirus à jour, changez régulièrement de mot de passe et ne préenregistrez pas vos identifiants de connexion et d'achat.



dernier rapport en date (2019), Marie-Christine Caffet, la médiatrice de la Fédération bancaire française, qui traite les dossiers d'environ 150 établissements, a dû traiter un cas dans lequel l'escroc s'est fait passer pour un conseiller de la banque.

Le numéro de téléphone correspondait à celui de l'agence. Pour autant, la médiatrice a considéré que le client était à l'origine de son propre préjudice « *car c'est lui qui a activé un nouveau service, sur une sollicitation d'un fraudeur qui a utilisé les données personnelles communiquées* ». Mais elle ajoute que « *l'apparence de régularité de l'appel reçu, émanant du numéro de téléphone de son conseiller, a pu facilement endormir sa vigilance, ce qui limite la gravité de son imprudence* ». La médiatrice a coupé la poire en deux, proposant qu'une partie seulement des montants détournés soit remboursée.

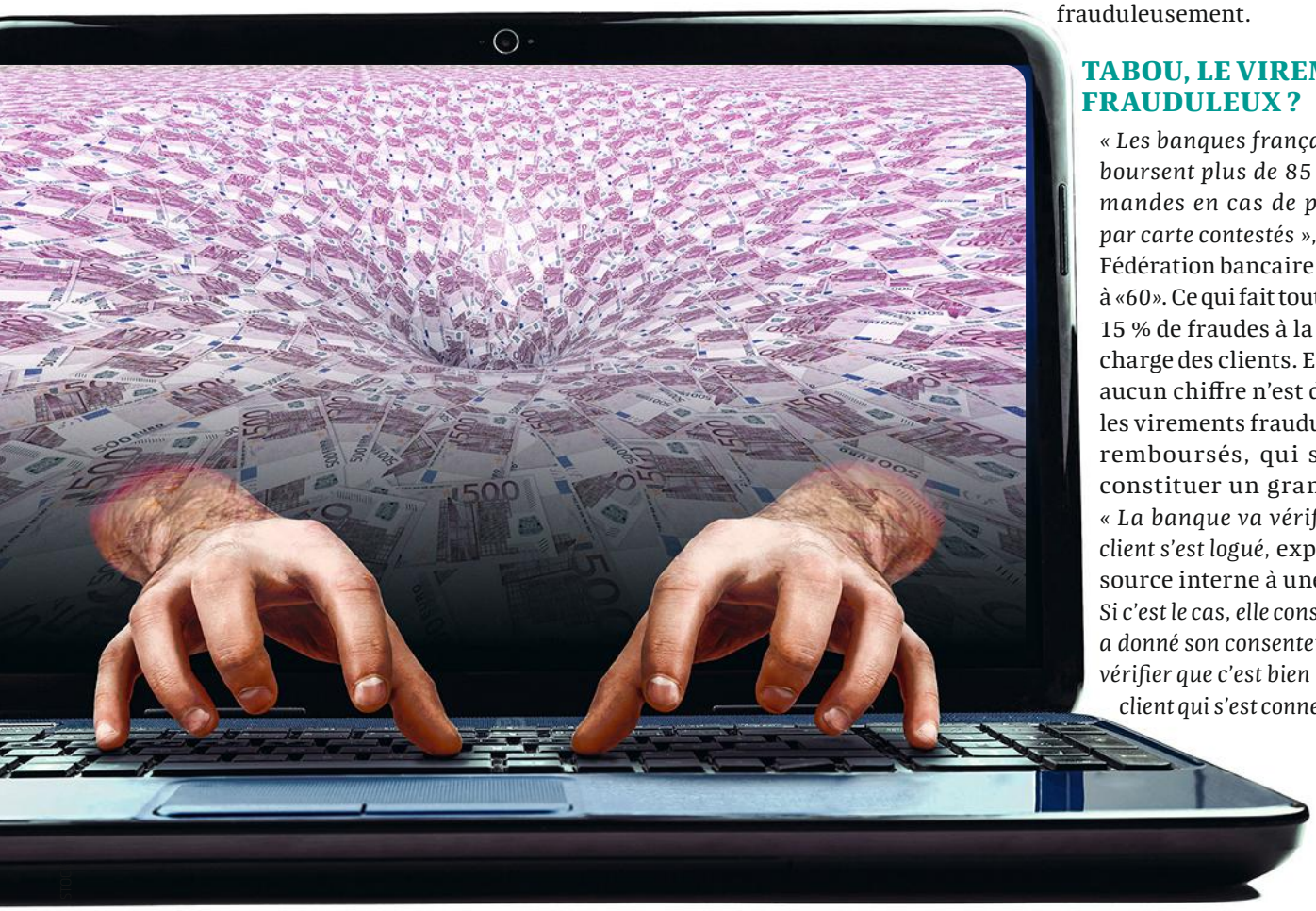
La seule solution, pour les victimes, consiste donc à assigner leur banque en justice. Le code monétaire et financier est clair : l'article L. 133-19 stipule que la banque doit rembourser toutes les pertes occasionnées par des opérations de paiement non autorisées.

> ***La seule solution pour la victime : assigner sa banque en justice.***

La banque qui refuse doit apporter la preuve d'une négligence grave du client. L'utilisation de l'instrument de paiement « *ne suffit pas en tant que telle à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant* » (article L. 133-23 du code monétaire et financier). « *Malgré ces dispositions du code monétaire et financier, les banques refusent de rembourser les victimes de virements frauduleux* », confirme Maître Katia Debay, avocate à Versailles spécialisée dans la défense des clients. Elle obtient régulièrement des jugements rétablissant leurs droits aux victimes, et condamnant la banque à rembourser les sommes virées frauduleusement.

BON À SAVOIR

Police et gendarmerie ont mis en place deux plateformes de signalements. Pour une arnaque sur Internet, connectez-vous sur Pharos. Prochainement, il sera possible de porter plainte en ligne. Pour une fraude à la carte bancaire, connectez-vous sur Perceval. À sa création en 2018, elle recevait 16 signalements journaliers, elle en a reçu près de 820 par jour en 2020.



TABOU, LE VIREMENT FRAUDULEUX ?

« *Les banques françaises remboursent plus de 85 % des demandes en cas de paiements par carte contestés* », plaide la Fédération bancaire française à «60». Ce qui fait tout de même 15 % de fraudes à la carte à la charge des clients. Et surtout, aucun chiffre n'est donné sur les virements frauduleux non remboursés, qui semblent constituer un grand tabou. « *La banque va vérifier si son client s'est logué*, explique une source interne à une banque. *Si c'est le cas, elle considère qu'il a donné son consentement sans vérifier que c'est bien le légitime client qui s'est connecté* ».

L'autre raison est financière. Le bénéficiaire d'un virement frauduleux étant souvent un particulier, en France ou à l'étranger, impossible pour la banque de récupérer les sommes détournées et donc de les restituer, contrairement aux fraudes à la carte. Car dans ce cas, les contrats bancaires des sites marchands prévoient que les sommes ayant servi aux achats frauduleux sont débitées du compte du vendeur par sa banque.

UN MODE OPÉRATOIRE QUI ÉTONNE ENCORE

Sur les méthodes employées par les escrocs, Marie-Christine Caffet, confesse son incompréhension. *« Le fraudeur s'immisce dans la banque en ligne de sa victime pour réaliser des virements après avoir ajouté son compte dans la liste des bénéficiaires (…). Le modus operandi des fraudeurs est encore assez mystérieux, notamment les intrusions dans les espaces en ligne, lorsqu'elles ne découlent pas d'un hameçonnage identifiable. »*, lit-on dans son dernier rapport. Interrogé, le régulateur du secteur bancaire donne davantage d'informations. *« Les fraudeurs collectent généralement ces données par des actes de piratage informatique : virus (pièce jointe ou clef USB piégée), phishing (envoi d'un faux mail ou SMS à l'effigie de la banque ou d'un créancier : opérateur téléphonique, fournisseur d'électricité…), arnaques téléphoniques ou sur Internet (appel usurpant l'identité d'un conseiller, faux placements…) »*, énumère ainsi le porte-parole de l'Autorité de contrôle prudentiel et de résolution (ACPR). Notre enquête montre l'existence d'une véritable chaîne commerciale du piratage. En haut de la pyramide, un hacker fait commerce de données bancaires qu'il a pu récupérer par ruse (phishing, usurpation d'iden-

Une véritable chaîne commerciale du piratage organisée.

Notre avis L'authentification forte protège-t-elle mieux ?

C'est un atout, mais aussi le prétexte de nouvelles tentatives de fraudes. Pour lutter contre cette escroquerie galopante, la deuxième directive européenne sur les services de paiement (dite DSP2) a rendu obligatoire une authentification renforcée du payeur, par carte bancaire ou par virement (donc *via* l'accès à ses comptes). La procédure 3D Secure, utilisée en France, ne repose que sur la possession d'un mobile, qui reçoit par SMS un code confidentiel à usage unique. Il faut désormais deux éléments d'authentification qui appartiennent à deux catégories parmi les trois suivantes (article L.133-4 du code monétaire et financier) :

UNE CARACTÉRISTIQUE personnelle

- Quelque chose que vous êtes le seul à connaître : un mot de passe, un code PIN, une information personnelle.
- Un objet que vous êtes le seul à posséder : un ordinateur, un téléphone, un bracelet connecté, un appareil fourni par votre banque.
- Un moyen de vous reconnaître, c'est-à-dire une caractéristique biométrique : votre empreinte digitale, le son de votre voix, la reconnaissance de votre visage.

LA VIGILANCE, composante essentielle

« Ce n'est toutefois pas une sécurité absolue, en particulier en cas de phishing actif ou de piratage de la ligne de téléphonie utilisée pour l'envoi des codes de validation par SMS, reconnaît l'autorité de contrôle du secteur (ACPR). *La vigilance des utilisateurs est une composante essentielle de la protection des accès à la banque en ligne ».*

COMMUNIQUER… avec votre banquier

La DSP2 peut être le prétexte à de nouvelles escroqueries. *« Les escrocs surfent sur toutes les actualités,* alerte le collectif banque de l'Indecosa-CGT. *Ils vous menacent de bloquer votre compte si vous ne répondez pas tout de suite, ils citent la directive… Ne cliquez sur aucun lien qui vous sera envoyé sous ce prétexte. Faites vous-même le chemin pour communiquer avec votre banquier. »*●

ISTOCK

tité), ou alors en s'introduisant dans l'ordinateur ou le smartphone de la victime par le biais d'un lien ou d'un SMS malveillant.

UN « ALLÔ » DE HACKERS QUI VOUS CÔUTE CHER

Damien Bancal, expert en sécurité informatique, a pu s'introduire dans l'une de ces boutiques virtuelles. « *Le* black hat *(hacker délinquant) possède plusieurs comptes, dont un sur la messagerie sécurisée Telegram. Dans ces espaces privés, on peut acheter, entre autres, des séries de données bancaires piratées et savoir comment les utiliser.* » L'expert a ainsi repéré le procédé dit du « *Allô !* », utilisé pour pirater les comptes bancaires *via* un appel téléphonique. « *L'escroc possède toutes les informations bancaires sauf une, le code dédié à la double authentification. Le "Allô" permet de le récupérer par téléphone.* »

Le guide pratique fourni par le hacker explique qu'il faut alors « *spoofer* » (usurper, en français) le numéro de l'agence bancaire. Cette technique permet de contacter la victime en affichant le numéro de la banque sur son écran. Le pirate n'a alors plus qu'à demander l'information manquante et le tour, malheureusement, est joué. « *Le "spoofing" revient en force depuis la mise en place de la double authentification* », observe Damien Bancal. Le hacker promet un taux de réussite de 80 % qui « *explique notre prix* » – jusqu'à 50 € le kit pour pirater un compte. « *Le commerce de données bancaires s'opère aussi, de plus en plus souvent, par Snapchat ou Whatsapp* », complète le capitaine de gendarmerie Arnaud Cheminant, responsable de la plateforme de signalements Perceval qui, depuis trois ans, date de sa création, réprime la fraude à la carte bancaire.

UNE RECOMMANDATION RESTÉE LETTRE MORTE…

Pour lutter contre l'intrusion dans les espaces en ligne, la médiatrice des banques a recommandé aux banques de vérifier auprès du client chaque modification intervenue sur les données de contact renseignées. « *Tout changement de numéro de portable, d'adresse mail, voire de code personnel doit être confirmé par deux moyens différents ; lorsque ces changements précèdent immédiatement la saisie d'un nouveau bénéficiaire de virement, les opérations débitrices doivent être gelées et leur consentement revérifié, par deux moyens différents.* »

Selon nos constats, cette recommandation figurant dans le rapport 2019 est restée lettre morte. Les établissements bancaires se contentent de campagnes de prévention. « *Une banque n'envoie jamais de lien de connexion, et ne demande jamais de communiquer ses coordonnées bancaires, par mail, téléphone ou message* », répète leur fédération. Alors que manifestement, les arnaques proviennent aussi d'autres sources qui sont moins identifiables.

Comme toutes les autres victimes, Yves attend toujours son remboursement. Il connaît le nom de sa bénéficiaire, sa ville, son agence bancaire. «60» a même pu la joindre, elle a déjà dépensé les 1 400 €… ●

LIONEL MAUGAIN

3 questions à

OMAR MERCHI
Commissaire de police*

Confirmez-vous la hausse des fraudes bancaires ?

OMAR MERCHI : Oui, elles ont progressé de 42 % au premier quadrimestre 2021 par rapport à celui de 2020. Ce type d'escroquerie, avec captation des identifiants et des coordonnées bancaires, se démocratise.

Comment opèrent les escrocs ?

O. M. : La première captation reste le courriel d'hameçonnage bancaire. Ce procédé s'est perfectionné en imitant parfaitement les messages de la banque et en faisant un renvoi vers un site frauduleux. Les victimes ne se rendent pas compte qu'elles ont cédé leurs données personnelles en cliquant sur un lien malveillant et elles sont persuadées d'avoir utilisé leur service bancaire habituel. Le second procédé consiste à s'introduire sur l'ordinateur ou le portable de la victime. Il suffit d'un mail qui n'a rien à voir avec la banque (publicités, opérateur de téléphonie…). En cliquant sur la pièce jointe, il ne se passe rien en apparence. En réalité, l'ordinateur va être infecté. L'escroc peut récupérer identifiants bancaires, mots de passe, logins lorsqu'ils ont été mémorisés. Puis Il revend ces données à une plateforme du *dark Web*. D'autres escrocs vont les acheter et les exploiter. Plusieurs semaines peuvent s'écouler entre la captation et la fraude perpétrée.

Comment démanteler les réseaux ?

O. M. : En mai, nous avons fait tomber une plateforme du *dark Web* qui commercialisait des kits de fraude, qui intégraient une solution permettant de contourner le système 3D Secure. Le prix de ces kits varie de 5 à 50 € en fonction de la qualité du produit.

* Adjoint au chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.