Face aux fraudes, LCL manque de crédit

Des clients de l'ex-Crédit lyonnais ont été plumés de plusieurs milliers d'euros chacun par des hackeurs. La banque refuse de rembourser la plupart des victimes, les accusant d'avoir été imprudentes et négligentes…

VICTIMES… et coupables de l'être ! Avec des sommes de 1 000 à 89 000 euros piquées sur leurs comptes, des clients de LCL, toujours plus nombreux, ont vite compris qu'ils étaient visés par une arnaque de taille. « Le Canard » a recueilli une trentaine de témoignages. La banque, elle, n'a pas tardé à tout mettre sur le dos des lésés.

Ces petits veinards ont subi des escroqueries entre novembre et avril dernier. Le mode opératoire ? Toujours le même. Des pirates ont infiltré leurs comptes via Internet et viré de grosses sommes à l'étranger. Certains clients ont reçu des SMS les avertissant de la transaction, d'autres ont tout simplement constaté, quelques jours plus tard, que leur compte avait fondu. Tous ont contacté leur agence pour demander un remboursement. Réponse ? Ces opérations frauduleuses n'ont été rendues possibles que parce que les titulaires des comptes, ces écervelés, avaient mal sécurisé leurs données !

Comme Michael Szalavecz, qui, à la réception d'un SMS suspect, a appelé illico son agence… Pas de chance : celle-ci n'a pas activé de protection sur son compte, lequel, peu de temps après, s'est trouvé délesté de 8 790 euros. Si les conseillers eux-mêmes sont censés recevoir une alerte à chaque activité suspecte sur leur portefeuille, aucun n'a bronché quand les 88 756 euros d'un autre client, Loïc Vidal, ont été virés à l'étranger.

Déplorables clients

LCL a adressé aux plaignants une lettre type plutôt lénifiante affirmant que la banque avait tenté d'organiser le retour des fonds – en vain. Après analyse du dossier avec ses « *experts* », ajoute LCL, le groupe a conclu, sans donner de détails, que les titulaires des comptes n'avaient pas été prudents. La loi est pourtant formelle : c'est à la banque de prouver que son client a fauté en refilant un code ou une info à un tiers.

« Le Canard » a posé la palme sur une fiche interne du Crédit lyonnais destinée aux conseillers. Elle rappelle qu'une suspicion de vol Internet doit être notée dans le dossier client et que « *la rapidité et la qualité du traitement d'une alerte permettent de mettre en échec les fraudeurs* ». Sans blague ? La victime doit ensuite porter plainte – ce qu'ont fait les clients dépouillés à Nice, à Roubaix ou à Lyon…

Et après ? « *Si le client demande à être remboursé au motif qu'il n'a pas autorisé l'opération ou qu'il remet en cause la sécurité du système informatique LCL*, [c'est niet ! Motif] : *"Il n'y a pas de faiblesse dans le système informatique de LCL."* »

Le fautif, c'est le ruiné ! Après avoir commencé, entre novembre et janvier dernier, à indemniser des plaignants, la direction générale, prenant conscience de l'ampleur du pillage, s'est ravisée, préférant laisser les râleurs se plaindre au tribunal.

Lâchés par leur banque

C'est aussi ce qu'a fait la BNP en décembre 2020, raconte Michel Guillaud, le président de l'association France Conso Banque, qui a vu débouler une vingtaine d'adhérents, tous plumés de 6 000 euros. L'établissement bancaire a reconnu la faille informatique et a commencé à rembourser… « *Jusqu'à ce que les plafonds de l'assurance* [souscrite par la banque] *soient atteints* », explique Guillaud, qui a engagé des procédures pour défendre les lésés… Toutes gagnées ! Le même vient de lancer un recours collectif contre LCL.

Le 28 juin, l'UFC-Que choisir a décidé de porter plainte pour pratique commerciale trompeuse contre 12 banques, refusant elles aussi de rembourser les victimes de fraudes. Expert en cybersécurité, Damien Bancal estime que LCL n'est pas plus mal protégé que les autres mais qu'il aurait dû repérer l'entourloupe, en raison des sommes concernées et des méthodes, reconnaissables.

Difficile, même pour les plus aguerris, de se prémunir de ces attaques. Les escrocs récoltent des données qu'ils revendent des mois voire des années plus tard. Comment se rappeler si l'on a répondu à un mail frauduleux ou participé à un concours foireux ?

Contacté par Julien Courbet (RTL, 21/6), LCL a demandé les dossiers concernés pour les (ré)étudier au cas par cas. « Le Canard », qui discutait déjà avec la banque, n'a plus eu de nouvelles depuis. Il avait pourtant utilisé des courriels sécurisés…

Fanny Ruz-Guindos

Nos pirates ont du talent

C'EST ENTENDU, le Crédit lyonnais n'a rien à se reprocher. Il a cependant tenu à dresser, dans un document interne, l'inventaire des fraudes susceptibles de vider les comptes de ses bénêts de clients :

- le « **phishing** » (hameçonnage) : faux e-mails ou SMS permettant de voler les codes d'accès des plus naïfs. Ne cliquez ni sur le lien ni sur la pièce jointe ;
- le « **swap** », ou détournement d'une carte SIM : il permet d'aspirer les SMS du titulaire d'un compte, voire d'appeler son conseiller en se faisant passer pour le client ;
- le « **spoofing** » (usurpation) téléphonique : un appel via un numéro qui semble provenir de la banque… Ne décrochez pas ! ;
- l'« **ingénierie sociale** » : se faisant passer pour un conseiller, un petit malin demande au client de confirmer ses identifiants ;
- le « **malware** » : un virus qui s'installe sur l'ordinateur ou le smartphone, permettant le vol et la revente des données ;
- le « **rançongiciel** » : il touche les professionnels, obligés de payer pour éviter que leurs documents n'atterrissent sur le Net, et que l'affaire ne tourne au « pas net ».