Attention à l'arnaque à la carte Vitale !

Méfiez-vous si vous recevez une demande de renouvellement par SMS. Il pourrait s'agir d'une escroquerie bien huilée, de plus en plus répandue, qui consiste à soutirer vos coordonnées bancaires en se faisant passer pour l'Assurance maladie, ou même pour votre banque.

ELIE JULIEN

ALORS QUE les escroqueries liées au compte professionnel de formation (CPF) semblent s'essouffler, un autre type de piège, à en croire les experts de Cybermalveillance.gouv.fr (dispositif national d'assistance aux victimes d'attaques en ligne), monte en puissance : l'arnaque au renouvellement de carte Vitale.

Revenue « à la mode » depuis plusieurs semaines, « elle est désormais la deuxième la plus répandue en France, toujours derrière celle du faux mail à la convocation pour pédopornographie », observe Jérôme Notin, directeur général de la plateforme Cybermalveillance.gouv.fr. Les messages de prévention des banques se multiplient. L'Assurance maladie et même les forces de l'ordre ont dû alerter face au développement de cette fraude. « Ça n'arrête pas, c'est l'arnaque qui revient le plus cette année. Les pirates achètent des kits clés en main, puis remboursée. Je vais contacter les enseignes », convainc le faux banquier. Laure reçoit alors des SMS de sa (fausse) banque confirmant ses achats et, un peu plus tard, d'autres lui signalant qu'elle est remboursée.

La maîtrise technique de ces cybercriminels, qui ont donc réussi à pirater les lignes téléphoniques qu'utilisent habituellement vos banques pour vous contacter, laisse sans voix. Dans les heures qui suivent, sur la même discussion SMS, le Crédit agricole, le vrai, lui annonce qu'elle est à découvert... « C'est hallucinant, les messages du pirate et de la banque s'entrecroisent sur la même conversation SMS. Et dire que je l'ai remercié, alors qu'il m'a volé 1 230 €... » s'irrite Laure. Les remboursements, eux, ne sont bien sûr jamais arrivés.

Même Strauss-Kahn s'est fait avoir

Mais à qui la faute ? Le Crédit agricole reconnaît « une forte recrudescence de l'usurpa-

DES MALFRATS BIEN PRÉPARÉS

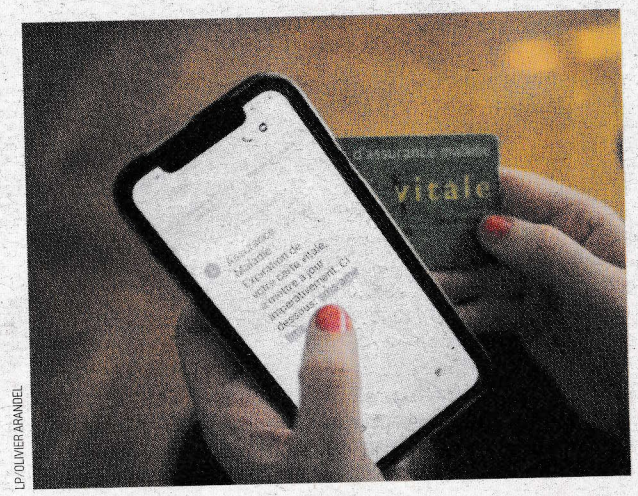
* *Confirmation par code secret ou sur application bancaire (directive européenne DSP2).*

> **Je ne me considère pas comme stupide, mais ils ont touché la corde sensible de la santé**
> LAURE*, 36 ANS, VICTIME QUI A PERDU PLUS DE 1 200 €

fraude. « Ça n'arrête pas, c'est l'arnaque qui revient le plus cette année. Les pirates achètent des kits clés en main, avec des sites très bien faits, sans fautes », constate Jean-Jacques Latour, expert de Cybermalveillance.

Laure*, 36 ans, commerciale en région parisienne, est encore sidérée d'en avoir été victime. « Je ne me considère pas comme stupide, mais ils ont touché la corde sensible de la santé », regrette celle qui a perdu plus de 1 200 €. Comme des millions de Français, selon les estimations de Cybermalveillance, la trentenaire a reçu un de ces fameux SMS l'invitant à renouveler sa carte Vitale.

« J'ai une ordonnance à renouveler régulièrement. Alors j'ai cliqué sur ce lien par SMS qui renvoyait vers un site très ressemblant à Ameli.fr *(celui de l'Assurance maladie)* », raconte Laure. Comme l'État a déjà pu envoyer des messages pendant la crise du Covid, elle ne se méfie pas. L'Assurance maladie rappelle pourtant sur son site qu'elle ne demande jamais d'informations médicales, numéro de Sécurité sociale ou coordonnées bancaires par SMS.



LP/OLIVIER ARANDEL

L'Assurance maladie rappelle qu'elle ne demande jamais d'informations médicales, numéro de Sécurité sociale ou coordonnées bancaires par SMS. *(illustration).*

Le signal d'alerte de pharmaciens et de médecins

Après avoir notifié son adresse postale, on lui demande de régler l'envoi de la nouvelle carte Vitale. Une somme dérisoire : 0,99 €. « Étrange de la part d'un service public », mais elle paye en entrant les informations de sa carte bancaire. Les jours passent et la carte Vitale n'arrive pas.

« Même si 1 % des personnes visées tombent dans le panneau, c'est énorme. Plus il y a de SMS envoyés, plus cela signifie que leur arnaque est rentable », déplore Jean-Jacques Latour. Signe qu'ils se multiplient, des pharmaciens et médecins doivent de plus en plus répondre « à des inquiétudes de patients ayant reçu ce message ». « C'est une hécatombe », souffle un médecin. « Les gens se méfient beaucoup moins des SMS », regrette-t-on à Cybermalveillance. Ce n'est pourtant que la première étape du piège.

Avec ses coordonnées bancaires, les voleurs passent à l'action. Après l'hameçonnage (ou phishing), place au spoofing, une technique qui consiste à appeler une personne en usurpant un autre numéro de téléphone. Dans les jours qui suivent, Laure reçoit ainsi des appels de différentes agences du Crédit agricole en Île-de-France, dont le nom s'affiche sur son écran. « Je suis affiliée en Haute-Garonne, donc je ne réponds pas à ces appels. Ce qui commence à m'inquiéter, c'est que je reçois des SMS d'alerte d'opérations frauduleuses sur mon compte bancaire alors que je n'y vois rien », se perd-elle.

Elle appelle sa conseillère. « Celle-ci m'explique que je ne dois pas tenir compte de ces SMS, qu'ils sont faux, poursuit la jeune femme. Le même jour, je reçois un nouvel appel du Crédit agricole Paris… » Cette fois, elle décroche, pensant que sa conseillère a signalé son cas. L'homme au bout du fil tombe bien.

« Bonjour, je suis du service de répression des fraudes du Crédit agricole », se présente-t-il, avant de lui poser quelques questions sur des achats suspects. « Avez-vous reçu un SMS pour la carte Vitale ? » l'interroge-t-il également. C'est alors que tombe son diagnostic : « Vous avez été piratée, comme des centaines de personnes, ne vous inquiétez pas. » Le discours de son interlocuteur, probablement lui-même derrière le faux message d'origine, est rodé. Il lui mentionne même ses identifiants bancaires qu'il a récupérés via le faux site Ameli. De quoi la rassurer.

Piégée, elle valide les achats du voleur

« J'ai l'impression d'avoir un employé de la banque. Il me dit qu'il va m'aider et passe une heure au téléphone avec moi », poursuit Laure, qui se sent aujourd'hui trahie. Si elle est ainsi contactée par son arnaqueur, c'est qu'il a besoin d'elle pour valider les dépenses qu'il a faites avec sa carte. En raison de la nouvelle directive sur les services de paiement de l'Autorité bancaire européenne (DSP2), les achats en ligne de plus de 30 € doivent en effet être confirmés avec un code secret ou sur l'application de sa banque.

Le voleur de Laure, bloqué par cette directive, lui demande de valider ses emplettes (chez Cultura, Back Market et Certideal) sur son application bancaire. « Vous serez débitée

* *Confirmation par code secret ou sur application bancaire (directive européenne DSP2).*

Mais à qui la faute ? Le Crédit agricole reconnaît « une forte recrudescence de l'usurpation de ses numéros en 2022 ». « C'est même devenu une part très importante de la fraude liée aux cartes bancaires », nous explique-t-elle. Insuffisant, pour Laure. La jeune femme a fait un signalement sur Perceval, site Internet qui permet de déposer une main courante et de signaler l'usage frauduleux de sa carte. « Ma banque a bloqué ma carte et, après étude, m'a annoncé qu'elle n'allait pas me rembourser en considérant que j'avais commis une négligence en donnant mes coordonnées bancaires », déplore-t-elle.

« La négligence des clients, c'est l'excuse numéro un des banques. Que l'on puisse vous appeler avec le numéro de votre banque, ce n'est pas normal », rappelle Jérôme Notin, qui incite les victimes à se rapprocher d'associations de consommateurs.

Bien ficelée, l'arnaque a fait une victime plus connue que Laure. L'ancien patron du FMI, Dominique Strauss-Kahn, a lui aussi été ciblé par de faux banquiers par téléphone. Un homme s'est fait passer pour le service de sécurité d'American Express afin de lui demander de confirmer l'achat d'une montre de luxe à 9 000 €. L'ex-cadre du PS s'est vu subtiliser au total la somme de 17 000 €.

* *Le prénom a été changé.*