Fraude sur Internet
LES QUATRE MENSONGES DES BANQUES

FACE À L'AMPLEUR DES ARNAQUES EN LIGNE, LES BANQUES RENÂCLENT À REMBOURSER LEURS CLIENTS. NOUS AVONS EXAMINÉ LEURS ARGUMENTS AVEC LE SERVICE JURIDIQUE DE «QUE CHOISIR». BEAUCOUP FONT FI DE LA LOI ET DE LA POSSIBILITÉ DE PIRATER LES DISPOSITIFS DE SÉCURITÉ !

ÉLISA OUDIN ILLUSTRATIONS **NINI LA CAILLE**

Les cyberattaques n'ont plus rien d'anecdotique. Grandes entreprises, PME, administrations, collectivités locales, particuliers: nous sommes de plus en plus nombreux à faire l'objet d'arnaques en ligne, notamment de paiements frauduleux. Selon le dernier rapport de la Banque de France, 1,3 million de ménages ont été escroqués en 2020, pour un montant total de 740 millions d'euros. Il faut dire que les hackers amateurs des premiers temps ont laissé place à des groupes mafieux expérimentés. *«L'ouverture du Web au grand public et le développement des cryptomonnaies ont accéléré la professionnalisation des attaquants. Des "start-up" du crime gagnent à présent assez d'argent pour se multiplier et devenir de véritables industries informatiques»*, indique Benoît Dupond, professeur de criminologie à l'université de Montréal, spécialiste de la cyberdélinquance. *«La criminalité va là où se trouve l'argent, et où le rapport bénéfice/risque est le plus intéressant. C'est le cas actuellement d'Internet»*, renchérit David Grout, *Strategic Advisor* chez Mandiant, société de cyberdéfense et filiale de Google.

En général, les escrocs ne travaillent pas isolés. Ils reçoivent l'aide de divers «fournisseurs», spécialisés dans une «branche»: vol des identifiants ou de cartes SIM, testing des données, recherche de vulnérabilité dans des applis de paiement... Des fuites chez Conti, considéré comme l'un des groupes criminels les plus actifs (188 millions d'euros de chiffre d'affaires estimé en 2021!), ont permis d'en explorer les coulisses. En un mois, de mi-novembre à mi-décembre 2021, il aurait mené plus d'une quarantaine d'attaques d'entreprises grâce à une centaine de salariés de toutes nationalités, en grande partie des experts du numérique mais pas uniquement. Conti (dont le site pro-russe a fermé en juin 2022) serait en effet très hiérarchisé, avec des métiers différents et des salaires en rapport, et œuvre de concert avec d'autres groupes comme Netwalker, LockBit, Ryuk et Maze. Ces échanges leur permettent de se tenir au courant des évolutions en matière de cyberprotection et de trouver de nouvelles failles. Certains achètent même des licences informatiques pour analyser les logiciels de sécurité et y encrypter leurs virus.

L'UFC-QUE CHOISIR AGIT

Autre caractéristique des malfaiteurs: leur rapidité d'intervention, sans doute liée au fait qu'ils ne s'arrêtent quasiment jamais. Group-IB, expert de la cybersécurité, a analysé les heures de travail chez Conti: *«Environ 14 heures par jour, sans jour férié (sauf le Nouvel An) ni week-end. L'activité commence à midi passé et ne décline qu'après 21 heures.»* Les banques, qui disposent de services de lutte contre la fraude numérique, sont au courant. Elles savent aussi qu'il existe de nouvelles techniques pour contourner l'authentification forte. Pourtant, nombre d'entre elles nient cette réalité et mettent en cause systématiquement, en cas de fraude, la responsabilité des consommateurs. Dans l'idée, bien sûr, d'éviter de les rembourser. À la suite d'une enquête mettant en évidence l'augmentation du nombre de refus de prise en charge, l'UFC-Que Choisir a déposé plainte contre 12 établissements, dont La Banque postale, le Crédit agricole, la Banque populaire, BNP Paribas, la Société générale et le CIC. Et voici une première mise au point juridique et technique pour que vous puissiez mieux vous défendre. ◈

AUTHENTIFICATION FORTE : COMMENT ELLE EST CONTOURNÉE

Ce système de sécurisation des paiements en ligne est basé sur deux étapes de validation, mais il n'est pas infaillible ! Nous listons ici les différentes méthodes des pirates pour tenter de déjouer le dispositif.

VOL DES IDENTIFIANTS DU COMPTE BANCAIRE

ATTAQUES CONTRE LE SITE DU COMMERÇANT

SPYWARE Un « logiciel espion » enregistre et fait fuiter toutes les données (notamment bancaires) des clients stockées sur le serveur du commerçant.

FORMJACKING Insertion d'un code malveillant sur les pages de paiement d'un site. Le pirate copie les données bancaires du client qui règle ses achats.

ATTAQUES CONTRE L'ORDINATEUR DU PARTICULIER

PHISHING Mail ou appel sous l'identité d'un organisme connu (impôts, Assurance maladie...) pour tromper un particulier et le conduire à livrer ses coordonnées.

MALWARE Infection d'un PC par un « logiciel malveillant » qui enregistre et renvoie aux pirates les données (notamment bancaires) du disque dur.

VOL DE DONNÉES OU DU CODE SMS

ATTAQUES CONTRE LE SMARTPHONE

PHISHING Mail ou appel sous l'identité d'un organisme connu (banque, fisc...) destiné à tromper un particulier ou un employé pour qu'il livre ses coordonnées.

INTERCEPTION DE SMS
Détournement de la carte SIM ou piratage du réseau de l'opérateur du particulier pour intercepter et dérouter les SMS qu'il reçoit.

1er mensonge

AVEC L'AUTHENTIFICATION FORTE, LA FAUTE VOUS INCOMBE

La quasi-totalité des opérations de paiement (par virement et par carte bancaire) est aujourd'hui soumise à un processus de validation dite « par authentification forte », ou « à double facteur ». Celle-ci fonctionne en deux étapes: dans un premier temps, le client doit renseigner ses données d'accès à ses comptes en ligne (identifiant et mot de passe). Ensuite, le plus souvent, il reçoit sur son téléphone mobile un code transmis par SMS afin de confirmer la transaction. La mise en place concrète de ce dispositif s'est étalée entre 2020 et 2022. En France, l'authentification renforcée est exigée dès le premier euro d'achat depuis le 15 mai 2021. Or, elle n'est pas sûre à 100%...

LES FAITS De nombreuses victimes se retrouvent dans la même situation que celle vécue par un client de Floa Bank le 15 août 2021. À la lecture de son relevé de comptes, ce dernier découvre que trois paiements en ligne ont été effectués avec sa carte bancaire auprès de Netflix, Orange Bank et Revolut. Le montant cumulé de ces achats atteint 1 513,99 €. Pourtant, le consommateur certifie n'avoir jamais autorisé ces opérations.

CE QUE DIT LA BANQUE Le service dédié à ce type de litige au sein de Floa Bank n'explique pas concrètement comment les paiements ont pu avoir lieu... mais il refuse de rembourser le client, au motif que *« la transaction a été réalisée sur un site nécessitant [son] authentification »*. Pour « prouver » la faute du consommateur, le conseiller bancaire lui fournit des pages de script informatique, évidemment totalement illisibles pour un particulier!

CE QUE DIT LA LOI Les banques appliquent l'authentification renforcée comme les y oblige la directive européenne de janvier 2018 (DSP2), mais les États membres de l'Union n'ont pas abrogé les dispositions en vigueur dans leur pays. Ainsi, en France, c'est l'article L. 133-23 du Code monétaire et financier qui détaille le partage de responsabilité entre les établissements et leurs clients en cas d'arnaque en ligne. Et il indique clairement que les premiers doivent *« fournir des éléments afin de prouver la fraude ou la négligence grave commise par les utilisateurs de services de paiement »*. Il ne pose nullement une présomption de culpabilité des consommateurs! Or, depuis la mise en place du dispositif d'authentification forte, certaines banques estiment que leur responsabilité se borne à prouver qu'elles l'appliquent. Cela équivaudrait à dire que la loi a été modifiée avec l'entrée en vigueur du système. ◈

Bon à savoir

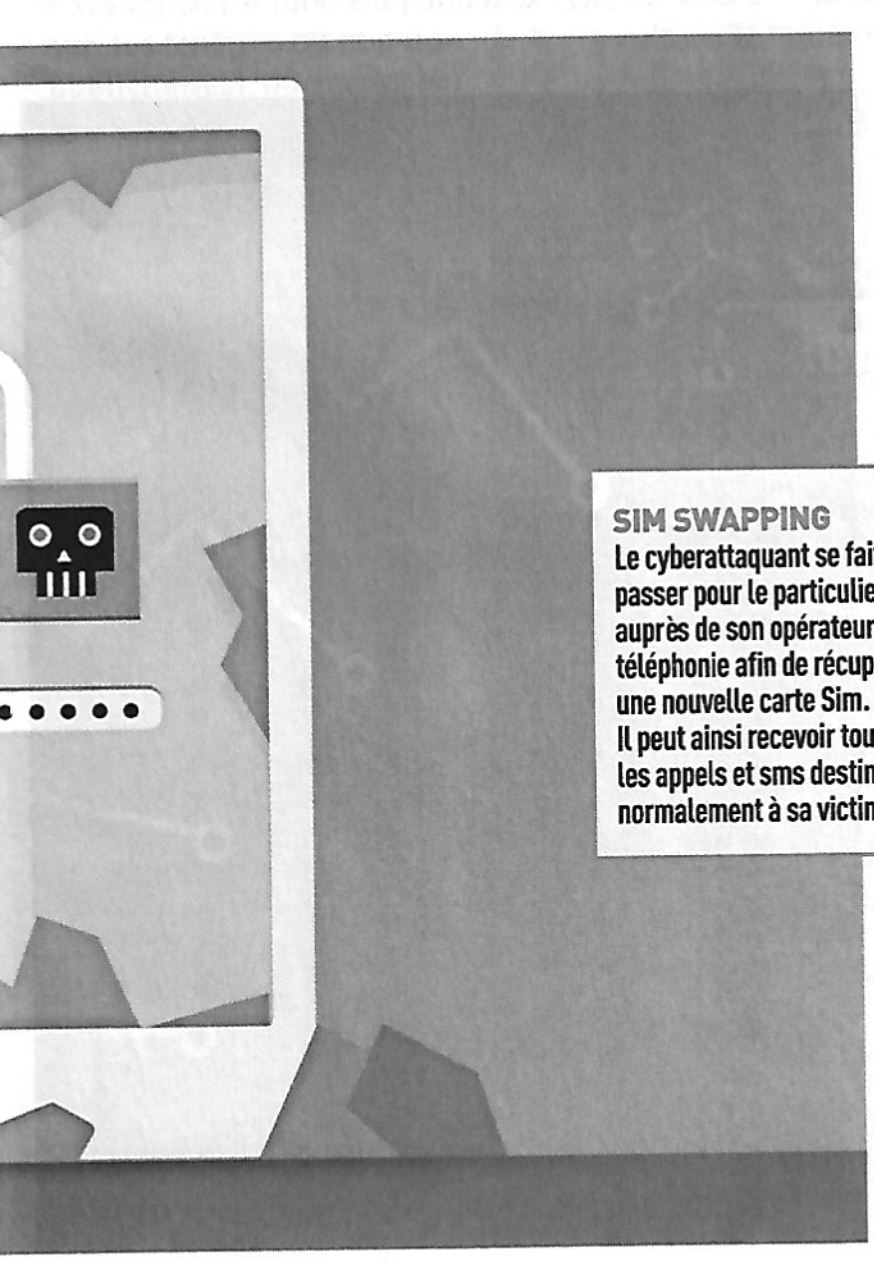
Une authentification forte ne vous a pas été demandée lors d'un paiement frauduleux ? La banque doit automatiquement vous rembourser. Ce cas particulier découle de l'article L. 133-19 du Code monétaire et financier, qui dispose que « le payeur ne supporte aucune conséquence financière si l'opération non autorisée a été effectuée sans que le prestataire de services de paiement n'ait exigé l'authentification forte du payeur, prévue à l'article L. 133-44 ».

2e mensonge

S'IL Y A FRAUDE, C'EST QUE VOUS AVEZ DONNÉ VOS CODES

Dans une majorité de cas aujourd'hui, si l'authentification forte a été mise en œuvre au moment de la validation d'un achat, les établissements financiers en déduisent que le titulaire du compte a forcément agi de lui-même, soit en rentrant ses codes sur l'interface de paiement, soit en les transmettant à un tiers – et tant pis si c'est malgré lui !

LES FAITS Le cas s'est présenté avec une cliente de la Banque populaire occitane. Le 4 avril 2021, elle reçoit quatre SMS pour confirmer deux demandes de virements en cours d'exécution, d'un montant total de 5 000 €. Elle contacte sa banque pour faire opposition. Mais cette dernière ne lui rembourse que 1 420 € (virés à une certaine Adeline Verpoorte), correspondant à la part des fonds ayant pu être rappelés. Le solde, soit 3 580 €, reste à la charge de la consommatrice.



SIM SWAPPING
Le cyberattaquant se fait passer pour le particulier auprès de son opérateur de téléphonie afin de récupérer une nouvelle carte Sim. Il peut ainsi recevoir tous les appels et sms destinés normalement à sa victime.

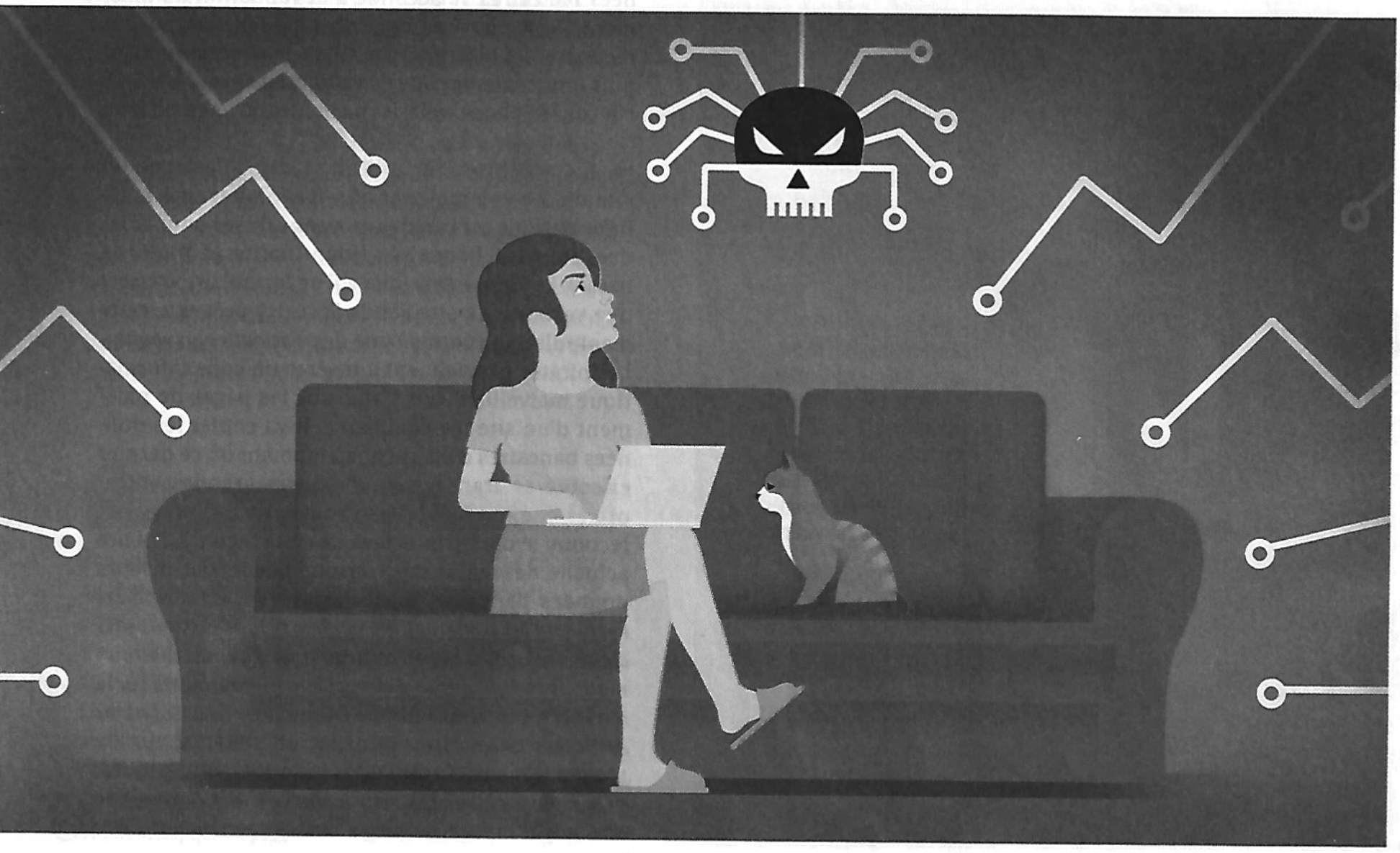
CE QUE DIT LA BANQUE La Banque populaire occitane refuse de payer les fonds non rappelés au motif que les virements ont été réalisés avec l'authentification forte. Elle précise qu'après vérification auprès de son service monétique, le code a été envoyé sur le numéro de téléphone de la cliente et utilisé pour valider le virement.

CE QUE DIT LA LOI La position des banques revient à affirmer que l'authentification renforcée est inviolable; or aucun des spécialistes en sécurité que nous avons interviewés ne valide cette affirmation. Certes, dans de nombreux cas, c'est la manipulation par du phishing qui conduit les clients à fournir leurs codes. Mais il existe également, aujourd'hui, des techniques criminelles qui n'impliquent aucune intervention de la victime. Pour mieux comprendre comment les fraudeurs opèrent, rappelons en quoi consiste l'authentification forte. Elle tient en deux étapes: la première vise à l'identification via les données bancaires, la seconde à la validation du paiement. Donc pour escroquer, les malfaiteurs doivent récupérer les informations relatives au compte client puis intercepter le code de validation envoyé par SMS sur son téléphone. Voici les méthodes qu'ils emploient.

→ **À l'occasion de l'identification** L'attaque du site d'un e-commerçant afin d'exploiter une faille informatique est l'un des moyens utilisés pour voler des données bancaires (identifiants et mots de passe). Le *formjacking* (ou « vol de formulaire ») en est une variante. Le site Panda Security présente cette manipulation comme l'une des *« attaques en vogue »*. Les pirates parviennent à insérer un code informatique malveillant (ou virus) sur les pages de paiement d'un site d'e-commerce. Il va copier les données bancaires d'un client au moment où ce dernier effectue sa transaction. Plusieurs grandes entreprises comme TicketMaster ou BritishAirways ont reconnu avoir été infectées de cette façon. À l'heure actuelle, des milliers de consommateurs ont eu leurs données bancaires ainsi « aspirées ». *« Des hackers exploitent les vulnérabilités des logiciels de certains sites d'e-commerçants moins sécurisés que d'autres. Les informations récupérées sont généralement revendues sur le darknet »*, confirme Phillipe Dubuc, *Principal Solutions Architect* chez Ping Identity, un fournisseur de moyens de sécurisation des identités numériques. *« On trouve aujourd'hui sur le darkweb les données de dizaines de milliers de cartes bancaires attendant d'être*

vendues pour quelques dollars puis exploitées au cours d'attaques potentielles », ajoute Valentine Ouaki, *Strategic Threat Advisor* à Crowdstrike. Identifiants et mots de passe peuvent également avoir été dérobés directement au titulaire du compte bancaire. Son ordinateur aura été infecté par un *spyware* (« logiciel espion ») ou *malware* (« logiciel malveillant »), qui s'y est installé sans se faire détecter. Il provient d'une pièce jointe, du téléchargement d'un logiciel infecté, de la consultation d'un site contaminé... Une fois en place sur le PC du particulier, il capte les données qui y sont enregistrées et les renvoie vers les pirates. Et n'oublions pas non plus les attaques par *ransomware* (autrement dit, la menace de publication d'informations contre rançon) dirigées contre les grandes entreprises. *« Les banques ne sont pas épargnées. Parmi ce qui leur est volé, il y a aussi des identifiants clients... »*, estime Raphaël Guérard, directeur Europe du Sud chez Forter, fournisseur de technologies de prévention de la fraude aux commerçants.

→ Lors de la phase de validation Une fois qu'ils ont les données du client en main, les pirates doivent encore se procurer le fameux SMS envoyé en cas d'initiation d'un paiement ou d'un virement – celui-ci est d'ailleurs souvent déclenché des semaines, voire des mois après le vol des identifiants. Ici sont utilisés le SIM *swapping* et l'interception de SMS. Dans le premier cas, l'escroc se fait passer pour le titulaire original d'une ligne auprès d'un opérateur de téléphonie, et prétexte que son smartphone a été perdu ou volé afin de récupérer une nouvelle carte SIM. Avec celle-ci, il reçoit tous les appels et messages destinés à sa victime. Europol a interpellé cette année 26 personnes, en Espagne et en Roumanie, qui s'étaient spécialisées dans cette méthode de fraude. Elles avaient dérobé près de 3,5 millions d'euros! La deuxième technique consiste à intercepter le texto comportant le code de validation envoyé au client. Elle est plus complexe, mais pas impossible. Selon le site de cyberdéfense Patrowl, les employés de la plateforme Twitter, qui reçoivent ce genre de SMS pour se connecter à leur session de travail, auraient été victimes d'une telle attaque. Les cybercriminels se seraient ainsi introduits dans le portail de gestion des comptes clients Twitter – il n'est pas exclu que les récupérations de codes aient aussi été, dans ce cas précis, réalisées par SIM *swapping* ou grâce à des complicités internes (ce qui n'est d'ailleurs pas exclu non plus pour les banques). ◈



NOS CONSEILS Limitez les risques de fraude bancaire en ligne

VOICI QUELQUES PRÉCAUTIONS UTILES POUR SE METTRE À L'ABRI DES TENTATIVES DE CYBERATTAQUES. BIEN SÛR, LA PROTECTION TOTALE N'EXISTE PAS. MAIS LES MESURES DÉCRITES CI-DESSOUS LIMITENT DÉJÀ DE FAÇON IMPORTANTE LE RISQUE DE VOL DE DONNÉES BANCAIRES.

ÉVITEZ DE TÉLÉCHARGER DES LOGICIELS ESPIONS

Les *spywares* qui contaminent les ordinateurs individuels sont susceptibles d'espionner et de voler vos codes de banque. Vous pouvez en télécharger, à votre insu, à partir de votre messagerie (en cliquant sur un lien dans un mail, en ouvrant une pièce jointe infectée), mais aussi via Internet (en consultant des sites piratés, en téléchargeant des logiciels vérolés, en cliquant sur des fenêtres ou pop-up publicitaires), ou encore par une connexion sur un disque dur ou un ordinateur contaminés (en utilisant une clé USB).
Pour vous en protéger, quatre mesures de sécurité s'imposent: ***1.*** disposer impérativement d'un antivirus et le mettre à jour régulièrement; ***2.*** n'installer que des logiciels de marque connue qui proviennent de source fiable; ***3.*** ne pas cliquer sur des pièces jointes ou des liens envoyés dans des mails à l'origine douteuse; ***4.*** naviguer en limitant les risques de contamination (c'est-à-dire sans visiter les sites à caractère pornographique, de streaming, de téléchargement illégal, de paris en ligne, etc.).

PROTÉGEZ-VOUS DU FORMJACKING

Ici, le vol des données bancaires a lieu au moment où vous effectuez un paiement en ligne. La protection la plus efficace consiste à utiliser le service d'e-carte bleue généralement proposé gratuitement par les banques. Cette carte bancaire virtuelle possède le même type d'identifiants (numéro, date d'expiration et code de vérification ou CVV), mais tous les chiffres sont renouvelés à chaque achat. Il est donc absolument inutile de les voler! Au minimum, si vous vous servez de votre carte classique sur un site marchand, vérifiez impérativement qu'il dispose bien d'une sécurité (c'est le fameux « s » après le http:// de son adresse internet qui fait toute la différence: https://). Et surtout, n'enregistrez jamais vos données bancaires auprès d'un e-commerçant (ni sur votre ordinateur d'ailleurs), même si cela vous est systématiquement proposé et présenté comme une solution beaucoup plus pratique!

ADOPTEZ LA PARADE AU PHISHING

La règle est simple ici, et doit devenir une véritable habitude: quelle que soit la raison pour laquelle vous vous connectez à un site internet, faites-le toujours en passant par Google et en rentrant vous-même l'adresse. Jamais en cliquant sur un lien. Il devient en effet de plus en plus difficile de savoir si les mails envoyés proviennent de sources authentiques ou non. Et, bien entendu, ne livrez sous aucun prétexte vos codes bancaires par Internet, SMS ou téléphone.

PRENEZ GARDE AU VOL DU SMS DE VALIDATION

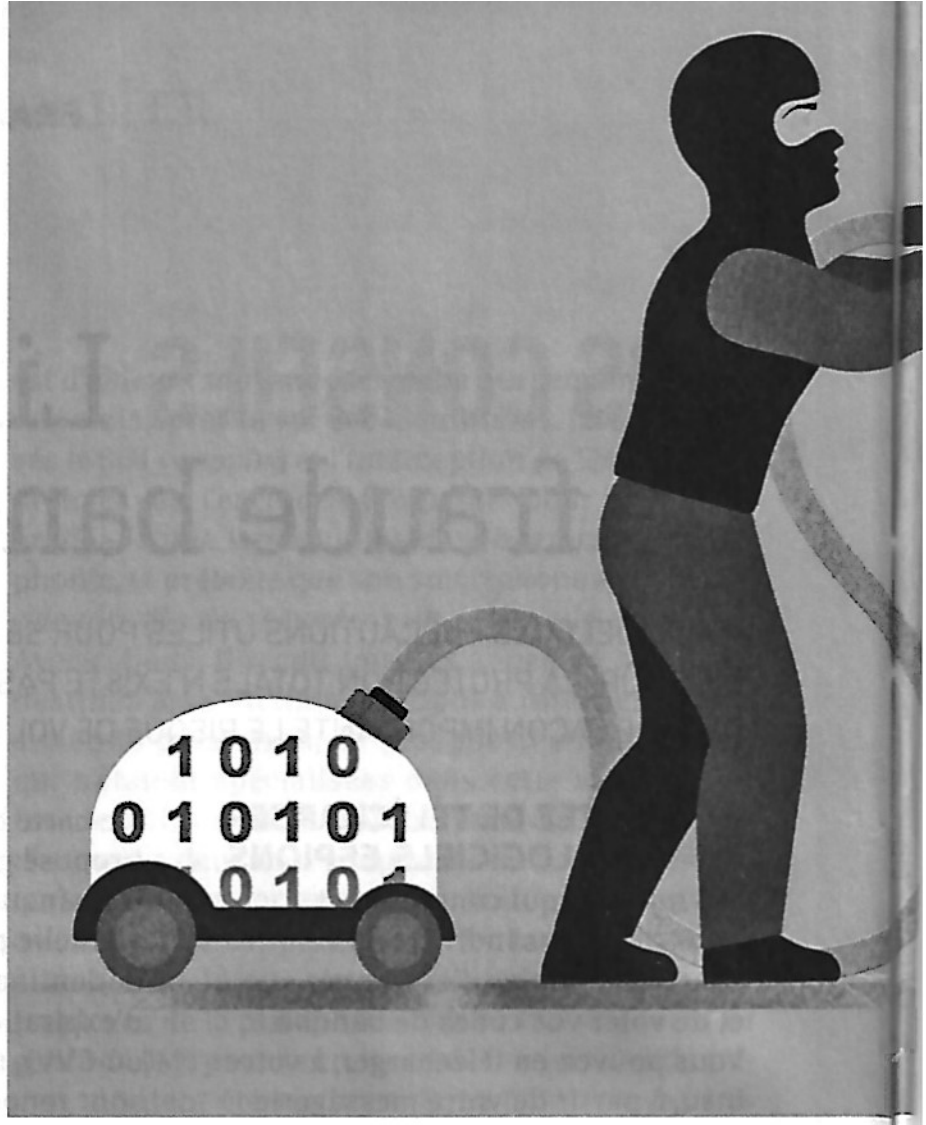
Il faut désormais veiller sur les codes contenus dans le SMS de validation comme sur ses codes bancaires. Ne les confiez jamais à distance, surtout à votre soi-disant conseiller bancaire.
Si vous constatez une interruption brutale de réseau sur votre téléphone mobile, vous êtes peut-être en train de subir une attaque par SIM *swapping* (lire aussi p. 52-53). Changez à l'instant même vos identifiant et mot de passe bancaires en vous rendant sur votre compte en ligne ou sur l'application de la banque. Puis, dans un second temps, modifiez tous vos autres mots de passe.

NE LAISSEZ PAS VOTRE PC ÊTRE INFECTÉ

Certains indices doivent vous alerter et vous conduire à vérifier l'état de votre ordinateur. Il devient soudainement lent, il ne s'allume plus ou alors difficilement? Des fichiers semblent modifiés ou supprimés? Des fenêtres publicitaires ou des messages apparaissent subitement à l'écran? Des mails sont envoyés sans votre consentement? Ces signes prouvent une infection. Là aussi, le réflexe est de changer immédiatement vos identifiants bancaires.
Mais cela ne suffit pas, il faut ensuite entièrement « nettoyer » votre ordinateur. Réalisez (ou faites faire) un scan complet de l'appareil pour trouver et supprimer les éventuels virus et *spywares*.

3e mensonge

EN CAS DE PHISHING, VOUS AVEZ ÉTÉ NÉGLIGENT



L'hameçonnage ou *phishing* consiste à obtenir, par la ruse, que le client livre lui-même ses codes. Cette technique continue d'être très largement employée par les cyberdélinquants. Elle s'est même particulièrement complexifiée depuis quelques temps. Dès lors, le particulier peut-il vraiment être mis en cause?

LES FAITS En 2020, une cliente de la Banque postale est victime d'une fraude particulièrement complexe. Le 4 septembre, elle reçoit un SMS qui l'informe d'un achat d'un montant de 500 €. Elle compose immédiatement le numéro de téléphone figurant sur ce SMS afin de signaler qu'elle n'est pas à l'origine de la transaction. Elle reçoit, dans la foulée, trois autres textos pour des achats, qu'elle dénonce également. Elle est pourtant débitée de 732 €. En réalité, le numéro indiqué sur le premier message n'émanait pas de sa banque, mais des fraudeurs. Pensant alerter celle-ci, la cliente est, en fait, entrée en contact avec eux et... tombée dans le panneau. Ces derniers ont joué sur la rapidité et l'effet de panique pour obtenir de la consommatrice qu'elle envoie ses codes, qu'ils ont utilisés pour les SMS suivants, correspondant, eux, à de véritables achats.

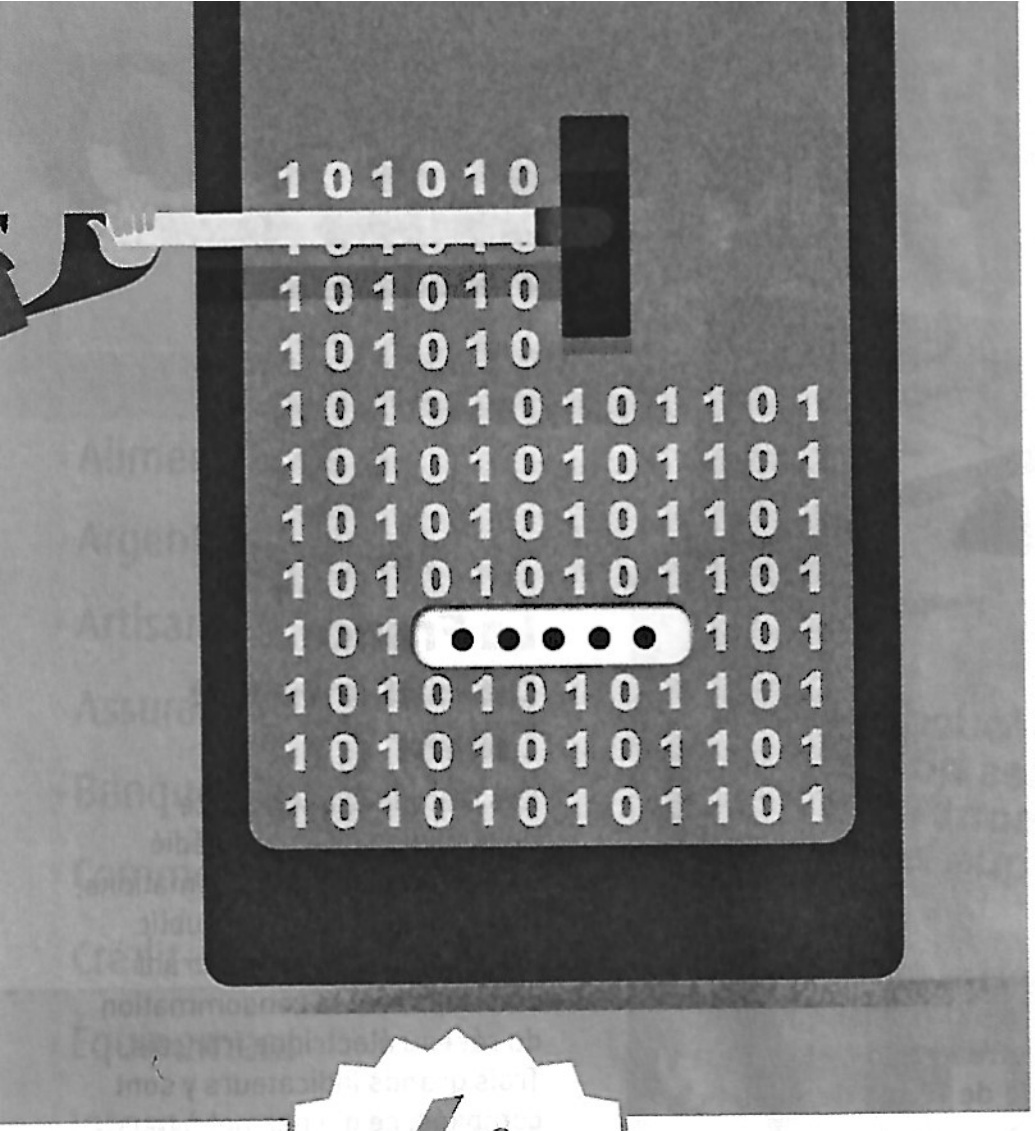
CE QUE DIT LA BANQUE L'établissement note que la consommatrice a été victime d'un stratagème (ou phishing) qui a permis aux escrocs d'obtenir ses données. Bien qu'il ne s'explique pas comment le premier SMS des fraudeurs a pu *«se dissimuler au beau milieu de la file des SMS envoyés par la Banque postale à la cliente pour authentifier de vrais paiements»*, il estime celle-ci responsable de négligence grave pour avoir livré ses codes.

CE QUE DIT LA LOI *«L'envoi d'un SMS d'alerte par les fraudeurs, qui porte le même numéro que ceux de la banque - ou d'autres organismes officiels (banques, services des impôts, Assurance maladie, police, etc.) - et qui vient s'intégrer dans la même file de conversation qu'eux, montre le haut niveau de technologie utilisé aujourd'hui par les cybercriminels. Et, par voie de conséquence, la difficulté à les différencier des vrais des faux SMS»*, souligne Philippe Dubuc, de la société Ping Identity. *«Les modes opératoires du phishing évoluent tous les jours. L'authentification forte a fait baisser le nombre de fraudes en 2021-2022, mais a également engendré de nouveaux types d'attaques, plus complexes»*, remarque Raphaël Guérard, directeur Europe du sud chez Forter. Les escrocs parviennent notamment à récupérer de plus en plus de données concernant leur victime (coordonnées, numéro de compte, nom du conseiller bancaire, etc.), ce qui leur permet d'installer un climat de confiance. C'est d'autant plus redoutable que les banques recommandent, en cas de fraude suspectée, d'agir très rapidement. Une autre technique consiste à dupliquer une application bancaire (même logo et présentation, etc.). *«Croyant être sur la véritable appli de sa banque, le client livre ses codes aux fraudeurs»*, indique David Grout, *Strategic Advisor* chez Mandiant. Précisons ici, comme le souligne Raphaël Guérard, *«que les employés de banques sont également victimes de phishing»*.

Ces méthodes, de plus en plus élaborées, interrogent sur la responsabilité du client. Peut-il être systématiquement taxé de «négligence grave», comme le maintiennent les banques, alors même que la fraude s'avère extrêmement difficile à détecter? Ce n'est généralement pas ainsi que pensent les tribunaux. La plupart des juges du fond donnent raison au consommateur, et la Cour de cassation a aussi bien précisé sa position en cas de phishing. Elle indique notamment, dans un arrêt de juillet 2020, qu'il faut déterminer si le client *«a commis une négligence grave en répondant à un courriel présentant de sérieuses anomalies tenant tant à la forme qu'au contenu du message»*. Ou si, a contrario, de telles irrégularités n'étaient pas observables, auquel cas il ne peut pas être accusé de négligence.

La position de la FBF

La Fédération bancaire française (FBF) rappelle que les banques déploient d'importants moyens contre la fraude. C'est vrai. La FBF estime aussi qu'un établissement a la faculté de refuser de rembourser son client si un «soupçon de fraude» pèse sur lui. Mais les termes de l'article L. 133-23 du Code monétaire et financier sont clairs : c'est bien au banquier «de prouver» la fraude ou la négligence grave du client. Il ne peut se contenter «de soupçonner»!



4e mensonge

LA BANQUE N'A PAS À MENER L'ENQUÊTE

Certes, un établissement financier n'a nullement la possibilité d'expertiser l'ensemble de la chaîne de paiement, et notamment l'ordinateur personnel d'un client. Mais ce n'est pas une raison pour prétendre que ce dernier a sciemment validé des paiements!

LES FAITS En avril 2020, un client de la Caisse d'épargne constate que plusieurs opérations frauduleuses ont été réalisées avec sa carte bancaire, via le dispositif d'authentification forte Secur'Pass. Il conteste être à l'origine de ces paiements auprès de sa banque, et précise habiter seul.

CE QUE DIT LA BANQUE Avec la méthode d'authentification renforcée, la fraude est impossible. Mais surtout, la banque n'a pas la capacité d'enquêter sur toute la chaîne de paiement (notamment sur le PC du client et le réseau internet). Donc, c'est à la police de mener les investigations, pas à elle.

CE QUE DIT LA LOI *«Une banque a la possibilité de voir si ses serveurs et/ou ses procédures de sécurité ont été mises en défaut. En revanche, elle ne peut pas, en l'état actuel des connaissances, savoir si l'ordinateur du client est compromis, car il faudrait une expertise directement sur son appareil. Et encore moins si c'est le réseau (Internet, mobile, etc.) qui l'a été, car il faudrait une expertise de l'exploitant»*, explique un informaticien travaillant dans une banque. Il existe donc toute une série de paramètres et d'inconnues. Le problème est que les banques s'en servent pour dire que la recherche de preuves prend fin à leur porte. Elles estiment que le reste relève d'une enquête de police. Peut-être, mais cet état de fait ne devrait pas être invoqué par les établissements financiers pour prétendre arbitrairement que le client est à l'origine de la manipulation, et qu'il a eu la volonté de procéder aux paiements contestés.◈

2 QUESTIONS À... Raphaël Bartlomé

Directeur du service juridique de l'UFC-Que Choisir

« L'analyse des médiateurs évolue »

QCA Pourquoi l'UFC-Que Choisir a-t-elle porté plainte contre les banques?
Raphaël Bartlomé Nous souhaitons mettre en lumière l'existence d'un véritable système faisant fi de la loi. Dans un certain nombre d'arnaques, les banques sont incapables de savoir ce qui s'est produit. Elles font alors peser les conséquences du vol sur le client, même si la fraude était indécelable par ce dernier. C'est en totale contradiction avec le Code monétaire et financier, qui dit clairement que la banque doit prouver la responsabilité du client.

QCA Y a-t-il déjà des avancées?
R. B. Oui, on constate que la communication commence à faire bouger des lignes. Sous l'égide de la Banque de France, un groupe de travail vient de se mettre en place pour réfléchir aux moyens d'améliorer le traitement des demandes de remboursement des clients. La commission européenne a été sensibilisée au dossier. Elle envisage de réviser la deuxième directive européenne sur les services de paiement (DSP2) concernant ce point. On voit aussi que certains médiateurs des banques font évoluer leur analyse, en prenant davantage en compte la charge de la preuve.