Nos comptes bancaires, cibles privilégiées des escrocs du web

19 mai 2021

Attention à nos comptes bancaires.
Les armes préférées des escrocs sont désormais notre téléphone et notre ordinateur.

Nous gérons désormais quasiment toutes nos opérations bancaires en ligne : nous consultons nos comptes, nous faisons des virements sur notre ordinateur ou notre smartphone. Nous achetons en ligne et payons à distance. La délinquance en ligne s'est organisée et elle est particulièrement active. Les arnaques financières évoluent sans cesse. La moindre faille du système, la moindre négligence du consommateur et ce sont des sommes considérables qui peuvent être détournées.

Nos opérations bancaires sont des données tellement sensibles qu'elles sont devenues les cibles privilégiées des cybercriminels.
Leur but : nous dérober nos identifiants de connexion de compte en ligne pour le pirater ou récupérer les coordonnées de notre carte bancaire, pour eux même ou pour les revendre.

La liste des arnaques est longue et les méthodes variées. Pour récupérer nos coordonnées, les fraudeurs sont capables de tout, y compris de fouiller nos poubelles (ayez le réflexe de détruire les documents comportant des informations confidentielles avant de les jeter pour empêcher toute usurpation !). Ils sont capables de nous observer pour récupérer notre code confidentiel et nous devons rester vigilants : **composez un code à l'abri des regards**, ne lâchez pas votre carte bancaire des yeux.

Mais les armes préférées des escrocs sont désormais notre téléphone et notre ordinateur. Ils s'insinuent dans notre boîte mail, nos textos, ils nous appâtent sur

les réseaux, les plateformes d'échange… Tous les moyens sont bons.

Quelques exemples :

 Un interlocuteur vous appelle, vous envoie un message et se présente comme votre banquier (ou autre.) … il aurait besoin du code confidentiel de votre carte bancaire sous un prétexte quelconque (problème technique, remboursement …). Retenez bien que votre banquier ne vous demandera jamais une telle information, il n'en a pas besoin. **Ne donnez jamais vos codes à qui que ce soit**. Ne donnez pas non plus les codes qui vous sont adressés par SMS, quoi qu'on vous dise….

 Les arnaques dites d'hameçonnage ou « phishing » sont toujours actives sur votre boite mail. Vous aviez appris à repérer les faux courriers bourrés de fautes d'orthographe, les escrocs font désormais des progrès. Ils continuent à imiter de vrais sites, même logos, mêmes présentations… (impôts, CAF, banque, opérateur de téléphonie etc.…), l'astuce consistant toujours à vous faire cliquer sur un lien.… Ne vous laissez jamais surprendre. On vous promet un important remboursement ? Pas question ! Reprenez la main, vérifiez l'information en cherchant le bon numéro de téléphone ou le courriel vous-même sur le véritable site. Restez aux commandes de vos déplacements en ligne.

 Vous proposez un bien d'occasion sur un site entre particuliers.… L'acheteur vous propose de vous envoyer plus d'argent que vous n'en demandiez et il vous demande de le rembourser… il veut des informations bancaires. Refusez tout « arrangement ».

 Vous recevez des publicités alléchantes. C'est le cas des propositions de crédit à taux défiant toute concurrence qui commencent par vous demander de virer des frais de dossiers. Pas question de céder à la « pression », un signe qui doit toujours vous alerter.

Bref, **pour toutes vos activités sur le web, vous devez ouvrir l'œil**. Vous jouez un rôle majeur pour protéger vos données bancaires.

Si un escroc prend la main sur votre compte, il peut faire de nombreuses opérations bancaires dans votre dos : Des virements à son profit, des achats à distance, lancer des prélèvements, ajouter un compte bénéficiaire, éditer des RIB. S'il vous vole vos informations personnelles, il peut les modifier et aussi changer les mots de passe.

Dans ce cas-là, il vous faudra réagir vite. **Vous contacterez votre banquier, pour faire opposition**, discuter des responsabilités, aussi. Car le client victime a des droits mais il a aussi des devoirs, notamment de vigilance, de prudence.

Quels sont vos droits ? Comment êtes-vous protégés ?

Le client a le droit d'exiger le remboursement des transactions frauduleuses qui n'ont pas été autorisées par lui quand sa responsabilité n'est pas engagée (article L 133-18 du code Monétaire et Financier). La banque doit rembourser immédiatement et remettre le compte dans l'état antérieur avec remboursement des frais, des agios et des commissions éventuels.
A défaut, elle doit démontrer que le client a commis des imprudences, fait une faute. Mais **elle a la charge de cette preuve** et démontrer « *que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre…* » sachant que » *L'utilisation de l'instrument de paiement ne suffit pas nécessairement 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* » (article L133-23 du code monétaire et financier).

Pour résumer, **la banque qui ne peut pas prouver la faute de l'utilisateur, supporte le risque**. Vous devez récupérer les sommes débitées et les agios éventuellement perçus.

Vous recevez un code par SMS pour confirmer l'ordre :

Nous connaissons, pour en avoir trop vu, des cas de fraude effectués à l'occasion d'achat à distance avec la carte. Pour aller au bout, l'escroc a besoin du code de confirmation arrivé sur votre téléphone. C'est pour ça que le fraudeur appelle en se faisant passer pour un conseiller bancaire (ou PayPal). Il prétexte avoir détecté une transaction suspecte et demande, pour y remédier, qu'on lui transmettre ce code qu'on vient de recevoir par SMS. Et le tour est joué.

Mais est-ce qu'un code envoyé par SMS suffit véritablement à protéger un consommateur en prouvant que c'est lui qui donne l'ordre ?

Plus maintenant. La deuxième Directive Européenne sur les Services de Paiement (dite DSP2) a rendu obligatoire la **mise en place d'une authentification renforcée**.

Or la procédure d'authentification « 3D Secure », utilisée jusqu'ici en France pour sécuriser les paiements en ligne, ne correspond pas au mode d'authentification forte requis par la DSP2. Car elle repose sur un seul facteur : la possession d'un mobile, qui permet de recevoir par SMS un code confidentiel à usage unique.

Il faut désormais deux éléments d'authentification qui appartiennent à deux catégories différentes de facteurs d'authentification parmi les trois catégories existantes (article L133-4 du code monétaire et financier), c'est à dire :

 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.

Attention : *il y a des exceptions pour les paiements de moins de 30 € mais à condition que le cumul ne dépasse pas 100 € sur une période que doit fixer la Banque. Et qu'on ne dépasse pas 5 opérations consécutives*.

Votre banquier n'aura pas manqué de vous rappeler cette obligation et d'insister pour activer cette authentification renforcée. C'est normal et tout devrait être enfin prêt en cette année 2021.

Mais là aussi, nous vous mettons en garde. Car les escrocs surfent sur toutes les actualités, pour vous prendre dans leurs filets. Ils savent vous rappeler l'obligation de souscrire à l'authentification renforcée, vous menacent d'un « compte bloqué » si vous ne répondez pas immédiatement, ils citent la Directive…Ne cliquez sur aucun lien qui vous sera envoyé sous ce prétexte, faites votre chemin vous-même pour communiquer avec votre banquier. C'est votre règle d'or.

Mais si le mal est fait, quels sont vos recours ?

Il faut réagir vite, prévenir la banque pour contester les opérations frauduleuses et demander le remboursement (sauf négligence prouvée par votre banquier). Attendez-vous à de la résistance sur ce terrain, mais ne cédez pas. **Vous garderez toutes les preuves**, les copies des messages malveillants. Si

la banque est fermée, usez des coordonnées dont vous disposez pour les joindre (téléphone, courriel.), pour démontrer à quel moment vous avez tenté de les joindre. **Vous confirmerez votre contestation par lettre recommandée avec accusé réception**.

***A savoir** : vous avez souscrit à une assurance pour vos moyens de paiement ? N'espérez pas une prise en charge en cas d'escroquerie sur vos comptes. Ce n'est jamais garanti.*

Le banquier vous demandera certainement de porter plainte. En fait, **ce n'est obligatoire que lorsqu'on vous vole vos moyens de paiements**. Ce ne peut être une cause de refus de prise en charge. Mais vous pouvez le faire, au commissariat ou à la gendarmerie, et signaler les faits à la **plateforme PHAROS**.

Sachez qu'en cas de débits frauduleux par carte bancaire, alors que vous l'avez toujours en votre possession, la réglementation est très protectrice pour le consommateur mais vous porterez plainte. Une fois la chose faite, vous signalerez l'escroquerie sur **la plateforme Perceval**. Le signalement facilitera le remboursement des sommes dérobées.

Les sites à connaître :

Vous pouvez consulter les listes noires et les alertes publiées par les autorités sur les sites internet :

* Assurance Banque Épargne Info Service (ABEIS) ainsi que l'Autorité des marchés financiers (AMF).

* Le site gouvernemental « Perceval » pour signaler des fraudes liées à la carte bancaire est accessible via Franceconnect. Il vous faudra l'identifiant et le mot de passe du site que vous avez choisi d'utiliser (impôts. Gouv, Ameli, …)

* Vous pouvez signaler des tentatives d'escroqueries par phishing sur la plateforme PHAROS (plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements), gérée par la police nationale et la gendarmerie nationale, elle est accessible sur le site www.internet-signalement.gouv.fr

* Vous pouvez obtenir des conseils et de l'assistance en appelant INFO ESCROQUERIES au 0811 02 02 17. Ou vous connecter sur le site cybermalveillance.

* Vous pouvez signaler les messages, spams ou sites douteux à Signal Spam. Si vous avez reçu le lien frauduleux par texto, faites-le suivre par SMS au 33 700. Pour faire bloquer ces messages.

Nos derniers conseils « pratiques » :

- Vous veillerez au paramétrage de votre ordinateur, à sa sécurité (antivirus et mises à jour).
- Vous éviterez le WIFI.
- Ne gardez pas vos mots de passe dans votre ordinateur et refusez toujours de les « enregistrer » pour faciliter vos connexions futures en consultant vos comptes ou sur un site commercial.
- Vous choisirez les mots de passe les plus complexes. « Un bon mot de passe doit contenir au moins 12 caractères et 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux » (CNIL).

Par le collectif Banque Indecosa CGT.