J'agis !

Liberté, Indépendance, Action

Sécurité bancaire : Barrez la route aux hackers !

Découvrez comment 2 nouvelles normes pourraient faire de votre compte bancaire la cible idéale des pirates du web !

Dans ce rapport inédit, vous allez pouvoir comprendre

- Pourquoi la menace est bien plus sournoise que vous ne pourriez l'imaginer
- Pourquoi un simple sigle sur votre carte bancaire pourrait tout changer pour votre sécurité bancaire
- Pourquoi votre argent peut littéralement s'envoler de votre compte sans que vous ne vous en aperceviez
- Pourquoi la nouvelle norme européenne sur les prélèvements bancaires pourrait donner le signal de départ à des milliers de pirates informatiques pour « *hacker* » votre compte
- Pourquoi en suivant 6 conseils concrets, pratiques et surtout applicables dès maintenant, vous pourriez vous éviter de vous faire dévaliser !

Menace n°1
Le Paiement sans contact

Menace n°2
Prélèvement SEPA :
encore une fausse bonne idée de Bruxelles...

Cher Lecteur,

J'ai une question pour vous : connaissez-vous vraiment votre carte bancaire ?

Au mois de juin dernier, l'émission *On n'est plus des pigeons* sur France 4 réalisait un mini-reportage sur le paiement sans contact. La jeune femme à l'écran demandait à des passants dans la rue s'ils connaissaient ce nouveau symbole présent sur de plus en plus présent de carte bancaire :

Personnellement, si je savais qu'il ressemblait au symbole du WiFi, je ne savais pas qu'il pouvait apparaître sur une carte bancaire !

Ni une ni deux, je vais chercher mon portefeuille, et là... surprise ! Je ne m'en étais jamais aperçue, mais ce symbole était bel et bien présent sur ma propre carte bancaire...

Pourquoi ce symbole pourrait tout changer pour votre sécurité bancaire

Alors... c'est quoi ce symbole ?
Comme nous le verrons plus en détail dans notre première partie, il s'agit du sigle du RFID garantissant à votre carte une nouvelle fonctionnalité : **le paiement sans contact.**

Apparue en 2010, cette nouvelle technologie appelée *Near Field Communication* ou NFC a, peu à peu, envahi nos portefeuilles. Elle vous permet de payer des achats de moins de 20 euros sans avoir à faire votre code secret. Il vous suffit en effet de simplement poser votre carte sur le terminal du commerçant. Aujourd'hui, et selon le Groupement des cartes bancaires CB, plus de 25 millions de cartes sont équipées de cette fonctionnalité.

Le premier problème, c'est que cette technologie vous expose à un risque que les banques semblent avoir négligé.

Les données passant de votre carte bancaire à la machine, dès qu'elles sont suffisamment proches l'une de l'autre, ces mêmes données peuvent être interceptées et détournées par une personne mal intentionnée... Avec un simple programme informatique que l'on trouve gratuitement sur Internet ou via une application à télécharger sur un smartphone, une personne malintentionnée peut dérober le numéro de votre carte bancaire et sa date d'expiration sans même que celle-ci ne quitte votre poche !

Une fonctionnalité qui vous est imposée... d'office par votre banque !

L'autre problème de ce type de carte, c'est que cette nouvelle fonctionnalité vous est imposée d'office par votre banque. En effet, comme nous allons le voir, votre conseiller ne vous laissera pas le choix et vous enverra par défaut une carte équipée de cette technologie lors de votre prochain renouvellement automatique de carte bancaire.

Conscientes pourtant des risques, et malgré les mises en garde de la CNIL, les banques sont prêtes à jouer à la roulette russe avec votre compte en banque... Il est donc temps de vous rebeller et d'adopter des mesures pour vous protéger ! Vous allez voir que en prenant des précautions toutes simples vous faites considérablement diminuer le risque de vous faire voler votre identité bancaire...

Mais hélas, comme nous le verrons dans notre seconde grande partie, j'oserais presque dire qu'il y a pire !

Vous avez sûrement entendu parler de la mise en place des **prélèvements SEPA.** Nous reviendrons en détail sur le principe de ces nouvelles normes exigées par l'Union européenne. Mais nous nous intéresserons surtout aux risques auxquels ce changement soumet votre compte bancaire. Car il vous expose à un risque tel... que je ne comprends pas qu'il ne fasse pas la Une du journal TV de 20 h !

Quand j'ai commencé mon enquête sur ce sujet, j'ai également commencé à en parler autour de moi aux *Publications Agora*. Et qu'il s'agisse de Cécile Chevré, rédactrice en chef de notre lettre *Croissance et Opportunités*, ou de Nathalie Boneil, notre responsable éditoriale, et même notre chère Simone Wapler – que l'on ne présente plus ! – auteur de trois bestsellers & rédactrice en chef de *La Stratégie de Simone Wapler* : toutes ont eu la même réaction : « *Mais pourquoi ont-ils mis un système aussi dangereux en place ?* »

La réponse vous attend dans quelques pages ; mais au-delà du pourquoi, il est surtout impératif de vous protéger... Et c'est pour cela que je vous donnerai quelques conseils à mettre en place dès maintenant pour parer les tentatives de fraudes.

Voilà, je crois que nous sommes prêts à commencer...

Menace n° 1 :
Le Paiement sans contact

Quel est le principe ?

Le principe est très simple : vous permettre de payer par carte bancaire plus rapidement, sans avoir à saisir votre code de sécurité. Plus rapide, donc plus sûr d'après les banques. Si vous avez une carte de ce type, tout est fait pour que vous puissiez vous servir de cette fonctionnalité au plus vite.

Pas d'abonnement, pas d'activation, pas d'autorisation à demander, vous pouvez à tout moment utiliser cette fonctionnalité de votre carte bancaire si celle-ci la prévoit.

Pour savoir si votre carte bancaire possède cette fonction, il vous suffit de regarder si le sigle du NFC est présent sur votre carte.

Source Visa

Si oui, vous pouvez donc payer vos achats d'un montant de 20 euros (maximum) sans insérer votre carte dans le lecteur, et sans composer votre code. Pour cela, il vous suffira de poser simplement votre carte sur le lecteur que vous présentera le commerçant.

En juin dernier, on comptait déjà plus de 25 millions de cartes de ce type sur l'ensemble du territoire.

Comment ça marche ?

Les cartes sans contact sont équipées d'une nouvelle technologie appelée NFC pour *Near Field Communication* (ou communication en champ proche). Il s'agit, résumé très simplement, d'une technologie permettant l'échange de données à moins de 10 cm, entre deux appareils équipés de ce dispositif.

Avec l'émergence des « objets ultra-connectés », le NFC est de plus en plus souvent intégré à la plupart des supports sous forme de puce. Ce type de puce équipant aussi bien les nouveaux passes de transports que certains passeports et maintenant donc nos cartes bancaires.

Source site du paiement sans contact

Pourquoi avoir créé une telle carte ?

On peut se demander pourquoi l'émergence de ces nouvelles cartes ? Les banques donnent trois raisons :

La praticité : oubliez les petites pièces au fond du portefeuille pour payer vos croissants le samedi matin. Vous pourrez payer ces petites dépenses du quotidien avec votre carte bancaire.

La rapidité : fini les longueurs, les hésitations au moment de faire votre code, il vous suffira de poser votre carte pour que la transaction soit enregistrée.

et enfin la sécurité : Aussi sûre qu'une carte classique, d'après les établissements bancaires, ce type de transaction éviterait que quelqu'un « voit » votre code... et donc diminuerait le risque de piratage...

Et pourtant, comme nous le verrons dans une minute, ce dernier point pose un gros problème.

Mais alors... où est le problème ?

Le problème réside dans la nouvelle puce qui équipe désormais ces cartes.

Si vous utilisez les transports en commun, vous êtes déjà familier avec le mode de fonctionnement des cartes équipées de puces NFC.

En effet, cette puce équipe déjà votre passe de transport vous permettant de simplement poser votre carte sur les

lecteurs pour voir les portes s'ouvrir devant vous.

Problème, ça ne sert pas qu'à faire biper et ouvrir les portes dans les couloirs du métro : ça enregistre aussi tout un tas d'informations... Si ces informations peuvent paraitre anodines pour votre passe de transport, elles le sont beaucoup moins lorsqu'il s'agit de votre carte bancaire.

Lorsque vous posez votre carte bancaire sur le terminal du commerçant, ce dernier interroge votre carte bancaire qui lui « répond » en lui donnant votre numéro de carte ainsi que la date de validité de cette dernière.

Et cela pose trois questions sur la sécurité de ces données :

1. À quelle distance votre carte émet-elle ?
2. Votre carte peut-elle être interrogée par une autre machine que celle de votre commerçant et ce, à votre insu ?
3. Les données de votre carte bancaire sont-elles cryptées ?

Des failles de sécurité béantes !

Le premier a avoir exposé le risque de cette technologie est Renaud Lifchitz, ingénieur chez BT (anciennement British Telecom). En 2012 lors d'une conférence *Hackito Ergo Sum*, il fait même la démonstration en direct qu'hacker ce nouveau type de carte est d'une facilité déconcertante, car :

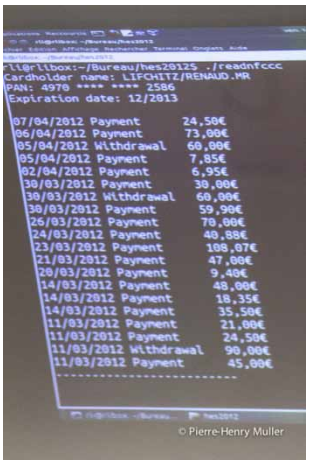
- d'une part la carte « répond » à toutes sollicitations et ce, même s'il ne s'agit pas d'un terminal de paiement chez un commerçant
- d'autre part les données émises par la puce ne sont pas cryptées !

Et nous verrons dans une minute que la distance à laquelle on peut interroger une carte dépend du matériel qui est utilisé pour interroger votre carte ! Pour le moment, revenons à la démonstration de notre ingénieur.

Lors de cette conférence intitulée *Hacking the NFC credit cards for fun and debit*, (traduction : hacker les cartes bancaires équipées de puces NFC pour le fun et l'arnaque), Renaud Lifchitz se posait une question très simple : Ma carte bancaire est-elle plus sécurisée que mon pass Navigo ?

Et la réponse aussi hallucinante soit-elle est NON !

Non, car comme va le démontrer l'ingénieur, non seulement votre carte bancaire ne requiert **aucune authentification** (il vous suffit de la poser, je vous rappelle), mais **les données qu'elle émet ne sont pas cryptées...**



L'ingénieur utilise une simple clé USB NFC (que l'on peut acheter sur le net pour quelques dizaines d'euros !) capable de capter les signaux émis par votre carte. Puis, après avoir téléchargé une application disponible gratuitement sur le net, la clé peut réceptionner et lire les informations transmises par la carte bancaire posée distante de quelques centimètres !

En 2012, l'ingénieur a pu ainsi capter le nom, le prénom du propriétaire de la carte, le numéro de la carte, la date d'expiration et même la liste des dernières transactions effectuées avec la carte !

Mais notre spécialiste va encore plus loin lors de cette démonstration, puisque comme il l'explique, toutes les cartes bancaires possèdent une bande magnétique, et une copie de cette bande est « stockée » dans la puce. Le problème est que celle-ci peut être interrogée via RFID c'est-à-dire à distance !

Ainsi il devient possible de faire cette même démonstration de hacking à distance avec un simple téléphone portable équipé d'un émetteur...

On pourrait donc tout à fait récupérer ces mêmes données sans même avoir à dérober votre carte avant !

On pourrait donc tout à fait récupérer ces mêmes données sans même avoir à dérober votre carte au préalable ! **Le vol des données bancaires se fait à distance.**

Renaud Lifchitz est effaré : « *La situation est ubuesque. Il n'y a aucune authentification, aucun chiffrement des données. Elles circulent en clair sur les ondes et on peut même y accéder avec une simple clé USB NFC ou un téléphone...* » L'ingénieur poursuit : « *Le protocole EMV (celui des cartes traditionnelles) a été repris tel quel et utilisé « dans les airs » sans se poser plus de questions* ».

Ainsi votre passe Navigo ou votre passe de transport est bien plus sûr que votre carte bancaire puisque lui utilise un **protocole de chiffrage avec un système d'authentification** pour ses communications !

Autre spécialiste, même constat : en 2012, Kristin Paget responsable sécurité et hacking chez *Recursion Ventures* **démontre lors de la convention** *Shmoocon*, qu'avec un petit budget pour s'équiper, il était possible de lire à distance le numéro ainsi que la date d'expiration de la carte bancaire de son voisin dans le métro ! En utilisant un lecteur RFID coûtant à peine 50 dollars, elle montre qu'il est même possible de procéder immédiatement à un paiement électronique avec ces données, via un appareil de magnétisation de cartes coûtant 300 dollars !

Oublier les 3 cm... Vos données peuvent être captées jusqu'à 15 mètres !

La même année, lors du congrès du Club des directeurs de sécurité des entreprises (CDSE), le commissaire de la Direction centrale du renseignement intérieur (DCRI) fait le même constat alarmant... Il va même plus loin puisqu'il explique qu'alors que les fabricants assurent que la lecture des données ne peut se faire qu'à trois centimètres d'une borne, il est en réalité possible de collecter ces informations à 15 mètres, soit 500 fois plus loin... avec le bon matériel. Une personne qui se tient à 15 mètres de vous peut pirater votre carte bancaire !

« N'importe qui pourrait scanner vos données bancaires, même à trois centimètres. Cela peut se produire facilement dans le métro, par exemple », explique le commissaire.

Depuis 2012, la CNIL s'est emparé du dossier et les choses ont bougé... un peu.

« Les tests réalisés […] ont permis de constater qu'il était possible de lire, avec un lecteur NFC (near field communication) indépendant ou intégré à un Smartphone standard, le nom du porteur de la carte bancaire, la liste des transactions réalisées, ainsi que le numéro de la carte et de sa date d'expiration »...

Mais « *des progrès ont été faits* », estime Gwendal Le Grand, chef du service de l'expertise informatique de la CNIL -- la Commission nationale de l'informatique et des libertés. Puisque la CNIL en collaboration avec le GIE des cartes bancaires (qui regroupent 130 établissements de crédits) a obtenu que les données personnelles comme le nom, le prénom et l'historique des transactions ne soient plus dans la liste des données accessibles via cette puce NFC.

Mais « certaines infos restent récupérables », relève Gwendal Le Grand ; ainsi le numéro de la carte et la date d'expiration sont toujours en libre accès pour les hackers...

Muni de vos données, rien de plus simple pour le hacker que d'aller faire un peu de shopping sur un site de e-commerce n'exigeant pas le cryptogramme (les 3 chiffres situé derrière votre carte), et de dépenser des montants qui vous feront blêmir... 500, 1 000 ou pourquoi pas 3 000 euros...

Et du côté des banques, on en dit quoi ?

Pour réaliser ce rapport, nous avons cherché à interroger plusieurs banques. Mais malgré tous nos efforts et des dizaines de sollicitations, personne n'a souhaité nous répondre.

Officiellement, les établissements bancaires nient les risques dont nous venons de parler.

Pourtant en coulisses, ils ont été contraints de faire des réserves **de protections spécialement créées pour ces nouvelles cartes afin de les rendre « hermétiques » au vol de données**. La Banque de France a expressément demandé à ce que les établissements s'équipent d'étuis de protection correspondant à hauteur de 10 % des cartes

NFC en circulation. Et ce pour parer à toute demande faite par leurs clients.

Du côté de la Banque de France, on tente de minimiser cette directive « *Ce n'est pas une obligation formelle. Cela fait partie de la politique de gestion des risques que chaque banque doit mettre en place et justifier* »...

Je vous livre ici le témoignage d'Isabelle : « *En rentrant de vacances, je découvre dans ma boîte aux lettres un courrier de ma banque me signalant que ma carte bancaire allait être renouvelée par anticipation, et qu'elle m'apporterait tout un tas de nouvelles fonctionnalités formidables, dont le paiement sans contact. Connaissant le risque afférant à ce type de carte, j'appelle mon banquier pour lui expliquer les risques liés au paiement sans contact et lui confirme que je n'accepterai sa nouvelle carte qu'à condition qu'il me donne un étui de protection contre le vol des données. Mon banquier tombant des nues me transmet son supérieur qui tombe tout autant des nues et découvre le problèmes. Il m'assure qu'il va « faire remonter le problème », qu'il n'a malheureusement pas d'étui à me proposer et qu'il ne peut donc rien faire pour moi... »*

Toujours d'après La Banque de France, ces 10 % d'étuis ne correspondrait pas au fait qu'un français sur dix encourt des risques de vol de données, mais seulement à un calcul de risque raisonnable... Les dirigeants craignant surtout une panique générale si des cas de fraudes étaient surmédiatisés

Les responsables craindraient surtout une crise de panique liée à un cas de piratage surmédiatisé par exemple.

Chez Visa, (*lire l'interview d'Albert Galloy responsable France du paiement sans contact un peu plus bas*), on relativise ces failles de sécurité : Certes ces données peuvent être hackées par une personne mal intentionnée, mais finalement ce sont des données qui étaient lisibles par tous puisqu'inscrites, sur la carte.

Une carte imposée par les banques...

Le vrai problème côté banque, est surtout l'attribution systématique d'une carte disposant de cette fonctionnalité du paiement sans contact à chaque client lors du renouvellement de celle-ci !

Que vous le vouliez ou non, votre banque vous fournira ce type de carte. Vous en avez peut-être même déjà une dans votre portefeuille !

La CNIL a récemment rappelé qu'il était indispensable que les titulaires de ces cartes soient « clairement informés de la fonctionnalité sans contact » et qu'ils puissent « la refuser, soit en obtenant une carte ne disposant pas de cette fonctionnalité, soit en obtenant sa désactivation par leur banque ». De même, la Banque de France impose aux banques de pouvoir disposer d'une procédure pour désactiver le NFC sur demande de la part de leurs clients.

Étant donné les risques de sécurité dont nous venons de parler, il est légitime de se demander pourquoi les banques persistent à fournir d'office à leurs clients ce type de carte sans contact et pourquoi elles ne font rien, ne serait-ce que pour crypter les données disponibles via la puce NFC. Car je vous le rappelle que ceci est tout à fait possible et déjà en vigueur par exemple pour les titres de transports (type Navigo) qui utilisent ces mêmes puces. Alors pourquoi ?

En un mot : **le coût !**

Et oui, votre banque sait que votre nouvelle carte vous expose à un risque de piratage, mais vous l'impose, car cela lui reviendrait plus cher que de demander à chaque client s'il souhaite ou non cette fonctionnalité sans contact.

Ainsi par exemple, le groupe CIC -Crédit mutuel qui s'est exprimé via son service presse :

« S'agissant d'un sujet de place concernant d'énormes volumes à traiter rapidement dans les villes tests, c'est la solution par défaut qui a été retenue sur le plan industriel pour minimiser les coûts. La gestion d'une interrogation préalable des porteurs est logistiquement et commercialement impossible, car d'un coût disproportionné. »

De même, des sécurités supplémentaires (cryptage ou chiffrage des données) ne sont pas installées, car elles feraient monter l'addition pour les établissements bancaires !

En résumé, alors que les failles existent, qu'elles sont prouvées, on préfère vous laisser dans l'ignorance et vous exposer à un risque de vol de données bancaires, (risque qui n'existait pas avec les anciennes cartes), **tout ceci pour optimiser les coûts**... *jusqu'à ce que des fraudes massives soient rendues publiques !*

En attendant... **votre carte bancaire est désormais une porte ouverte sur votre compte en banque pour les hackers !**

Interview d'Albert Galloy, responsable innovation VISA

Parlez-nous du paiement sans contact...

Le paiement sans contact répond à un besoin de simplifier les petits achats de la vie quotidienne. Grâce à ces nouvelles cartes équipées d'une puce NFC, vous allez pouvoir payer votre baguette chez le boulanger, vos courses chez votre boucher... L'idée était vraiment de créer un produit flexible qui puisse améliorer le quotidien des utilisateurs de cartes bancaires. Posez et c'est payé !
Pour les commerçants aussi, l'avantage est important puisque le temps de transaction est raccourci, les achats sont plus fluides. C'est un vrai gain de temps.

Mais que se passe-t-il si on me vole ma carte ? On peut donc faire des achats frauduleux puisque l'on ne me demande plus mon code pour valider la transaction ?

Techniquement oui. Mais il faut bien comprendre que le montant des achats ne peut pas être supérieur à 20 euros... et que selon les banques vous ne pourrez pas dépasser un certains plafonds pour vos paiements sans contact. De plus des contrôles de sécurités aléatoires peuvent être effectués se traduisant par une demande de la part du terminal de paiement lors de laquelle vous devrez introduire votre carte et composer votre code secret pour valider la transaction.
Dans tous les cas, sachez que ce sont les banques qui assument les risques puisqu'elles prendront en charge tous les achats frauduleux qui pourraient être fait en cas de vol de carte bancaire.
La peur que suscitent ces cartes bancaires est surtout liée à la nouveauté...

Démonstrations à l'appui, des voix s'élèvent pour dénoncer les failles de sécurité des cartes sans contact permettant un piratage à distance... on pourrait donc nous voler notre numéro de carte sans même qu'elle ne sorte de notre portefeuille...

Oui, je vois de quoi vous voulez parler. Cependant toutes les données qui pourraient éventuellement être récupérées sont déjà visibles à l'œil nu sur les anciennes cartes bancaires. N'importe qui auparavant pouvait en un simple coup d'œil voir le numéro de carte et la date d'expiration inscrits sur le recto de votre carte. Il n'y a pas plus de risque maintenant qu'il n'y en avait...

Pourtant, même les plus hautes instances comme la CNIL ont dû intervenir pour demander un renforcement de sécurité pour ces cartes... Concrètement peut-on avec le bon équipement capter le numéro de la carte bancaire et la date d'expiration ?

Oui, ces données sont captables. Mais elles sont inutilisables, puisque sur une majorité de sites internet, on vous demandera le cryptogramme [NDLR les trois chiffres inscrits derrière votre carte]. Le vrai travail va être de sécuriser Internet afin de rassurer les gens sur les paiements en ligne.

Certes, mais pour l'utilisateur de carte, ces informations ont de quoi faire peur. On peut me voler une partie de mon identité bancaire sans que je m'en rende compte. Pourquoi ne pas crypter les données émises par la carte comme c'est le cas pour les passes de transports ?

Nous avons souhaité créer un produit en privilégiant la flexibilité sans pour autant négliger la sécurité. Mais nous ne cryptons les données, car nous n'avons pour le moment pas constaté de cas de fraude avéré. De plus, le cryptage augmenterait les coûts à la fois pour le commerçant et son terminal de paiement, et pour les banques qui, pour le moment, peuvent donc offrir ce service à leurs clients.

Pourquoi ne pas simplement avoir laissé le choix au consommateur de prendre une carte avec ou sans cette fonctionnalité de paiement sans contact ?

Parce que si on attend les gens, on ne fait jamais rien ! Il y a eu quelques essais à plus petites échelles, mais cela ne fonctionnait pas. Mais on s'est aperçu qu'en mettant le produit entre les mains des utilisateurs, ces derniers étaient séduits.

Vous avez quelques conseils peut-être pour rassurer les gens qui auraient déjà reçu cette nouvelle carte ?

Premièrement, on voit sur internet des gens percer leur carte bancaire pour soi-disant « empêcher les transmissions » : c'est une folie. Sachez qu'en faisant ça, vous perdriez toutes assurances comprises dans votre contrat de carte.
Si vous souhaitez vraiment ne pas utiliser ce service, demandez à votre banque de désactiver ce service. C'est tout à fait possible.
Certains étuis peuvent également protéger votre carte et vous rassurer.
Enfin dernier conseil, sachez qu'en mettant deux cartes équipées de puces NFC côte- à-côte, *vous brouillez toutes les données qui pourraient être captées !*

Votre stratégie antivol de données...

REGLE NUMERO 1 :
Glissez votre carte dans votre étui !

En vous abonnant pour recevoir ce rapport, **nous vous offrons un étui protecteur** utilisant une technologie capable de bloquer les signaux émis par votre carte bancaire. La société française qui produit ces étuis de protection utilise un film de conception allemande (Cryptalloy) qui bloque efficacement les ondes (de 125 kHz à 800 MHz) émises par les puces.

REGLE NUMERO 2 :
Surveillez attentivement votre relevé de compte.

Votre relevé de compte sera désormais votre plus fidèle allié pour traquer les mouvements suspects sur votre compte. En gardant soigneusement TOUS vos tickets de cartes, vous pourrez pointer chaque dépense pour être sûr de son origine. N'hésitez pas à contacter votre banque en cas de doute ! Cette tâche, certes fastidieuse, s'avéra maintenant plus que jamais vitale pour la sécurité de votre compte en banque.

REGLE NUMERO 3 :
Demandez à désactiver le paiement sans contact

Attention, si beaucoup de banques vous proposeront de désactiver la fonction de paiement sans contact gratuitement, pensez à leur demander une nouvelle carte sans cette puce.

Un conseil, si votre banque a renouvelé votre carte bancaire en incluant d'office cette fonctionnalité paiement sans contact, sachez que vous pouvez déposer une plainte à la fois auprès de la CNIL, mais également auprès de la DGCCRF (répression des fraudes) puisque cette opération a donc été faite sans votre accord !

Menace n° 2
Prélèvement SEPA : encore une fausse bonne idée de Bruxelles...

Qu'est-ce que SEPA ?

Vous avez forcément déjà entendu parler du SEPA sans vraiment vous arrêter sur ce que signifie cette nouvelle norme. Si vous avez tendu l'oreille, vous avez peut-être compris qu'elle concernait vos prélèvements. Mais comme tout ce que fait Bruxelles, comprendre cette nouvelle réglementation causerait une migraine à la plupart d'entre nous.

Pourtant il est essentiel de s'y intéresser de plus près. Car au même titre que les cartes bancaires sans contact, SEPA expose votre compte bancaire à des risques de fraudes insidieux.

SEPA est le nom de la **réforme européenne sur les prélèvements bancaires**. SEPA signifie *Single Euro Payments Area*, ou si vous préférez espace unique de paiement en euro.

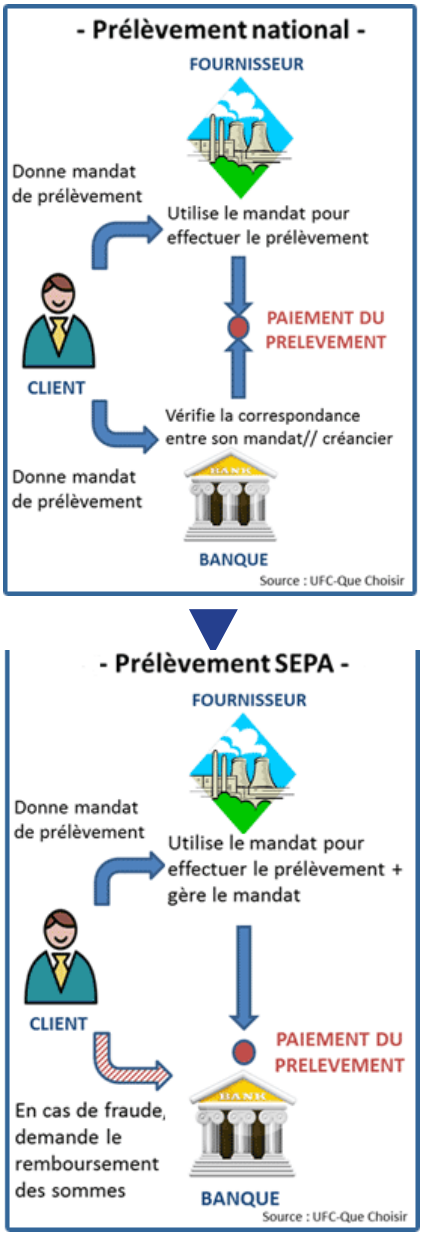
SEPA
Single Euro Payments Area
Espace unique de paiement en euros

Cette nouvelle règlementation est entrée en vigueur le 1er aout 2014 et vise à uniformiser les conditions pour tous les prélèvements effectués en euro au sein des 28 pays de l'Union Européenne mais également de la Suisse, de la Norvège, de l'Islande, du Liechtenstein et de Monaco.

Le but derrière cette réforme ?

Rendre ce moyen de paiement plus sûr et moins couteux pour les 380 millions de consommateurs. La promesse de Bruxelles réside dans l'idée qu'il n'y a plus de « *différence entre paiements nationaux et paiements transfrontaliers* », que ce soit en termes de coût ou de délais d'exécution...

Ce que cela va changer pour vous ?



Concrètement pour vous, il y a peu de changement... tout du moins en surface ! En effet, pour les créanciers à qui vous avez déjà donné votre accord pour effectuer un prélèvement sur votre compte, il n'y aura aucune répercussion. EDF, GDF, France télécom continueront à vous prélever sans que vous ayez besoin d'intervenir. Ces prélèvements seront automatiquement convertis pour s'adapter à cette nouvelle norme, sans frais pour vous.

À retenir : Si votre banque vous facture : demandez immédiatement un remboursement ! L'opération doit être gratuite.

En revanche, pour la mise en place d'un nouveau prélèvement, les choses changent légèrement. En fait, cela sera beaucoup plus simple :

En effet, **vous n'aurez plus à signer un document qu'il faudra ensuite envoyer à la banque pour autoriser un nouveau créancier à effectuer un prélèvement.**

Il vous suffira de signer le document remis par ce nouveau créancier et l'accompagner d'un RIB, votre créancier se chargeant de contacter votre banque pour faire effectuer le prélèvement.

Même chose pour révoquer un prélèvement existant :

Avant il vous fallait contacter à la fois votre banque et votre fournisseur (ou créancier). Désormais, il vous suffira d'envoyer une lettre recommandée à votre fournisseur (créancier) pour demander la résiliation de ce prélèvement.

Sur le papier, SEPA est donc un gain de temps pour vous. Sauf que ce mandat unique pose de sérieuses questions quant à la sécurisation de votre compte en banque.

Réfléchissez-y. Certes remplir et envoyer votre document prenait jusqu'ici un peu de temps, néanmoins **le pouvoir de demander l'exécution d'un prélèvement était dans vos mains !**

Et c'est bien tout le problème que pose le SEPA. **Car le pouvoir passe de vos mains à celui de votre créancier qui, muni de votre RIB, peut donc seul demander le prélèvement de votre compte.**

Évidemment si le créancier est honnête, il n'y a pas de problème. Mais ce type de procédure signifie qu'un malfrat ayant mis la main sur votre RIB pourrait faire main basse sur votre compte !

Et si vous pensiez que SEPA allait faire baisser vos frais bancaires, vous allez être déçu !

Même si la directive émise par Bruxelles affirme que les services de paiement « devraient [notez le conditionnel !] représenter un progrès sensible en termes de coûts pour le consommateur, de sûreté et d'efficacité par rapport aux systèmes existants au niveau national », vous pourriez voir apparaître de nouveaux frais aux intitulés nébuleux ces prochains mois.

En effet, pour réaliser la mise en place de SEPA, les établissements bancaires ont dû investir massivement pour être capable de traiter des demandes de prélèvements internationaux... et ces investissements d'une manière ou d'une autre seront répercutés sur le coût de votre compte en banque ! De même, les banques exigeaient auparavant des frais pour la mise en place ou la révocation d'un prélèvement (8 euros en moyenne !). Les banques sont donc en train d'inventer tout un tas de « petits frais annexes » visant à récupérer leur pécule !

Un bon conseil : Surveillez bien votre relevé, vous verrez...

Mais si le risque caché derrière SEPA ne résidait que dans cette hausse de coût, au fond, cela ne sera pas aussi problématique que ce à quoi nous devrions assister dans les mois à venir...

Le SEPA : fraudes, détournements et vol d'identité, un rêve pour les cybercriminels !

En quoi votre sécurité va-t-elle être compromise ?

Comme nous venons de le voir, **ce mandat unique transfère un pouvoir qui était entre vos mains pour le mettre dans celui de votre créancier... et votre intermédiaire n'est plus votre banque, mais bel et bien le bénéficiaire !** Et pour accéder à sa demande de prélèvement, votre banque ne vous contactera pas, elle ne vérifiera pas son authenticité, elle exécutera SA demande et non plus la vôtre.

Ainsi un cybercriminel ayant mis la main sur votre RIB (en piratant par exemple les données fournies à votre opérateur téléphonique), pourra présenter un mandat de prélèvement à votre banque en imitant votre signature... et se faire payer directement !

Un risque d'autant plus important que cette fraude peut venir de n'importe quel pays européen...

La nature même de cette réglementation est un vrai *pousse au crime* pour toutes les mafias européennes.
Retenez bien cette donnée importante : vous n'êtes plus la seule personne à pouvoir autoriser un prélèvement sur votre propre compte bancaire !
Bien sûr, il y a tout de même quelques « petites sécurités », mais elles sont tellement minces que n'importe quelle mafia pourra immédiatement les contourner...

Le créancier qui émet cet ordre de prélèvement devra avoir un identifiant ICS Identifiant Créancier SEPA) obtenu auprès de la Banque de France... Une précaution certes, mais qui n'est nullement une garantie de sécurité !

Ainsi n'importe quelle mafia pourra créer une micro société en Slovaquie, acheter une liste de Relevés d'identité bancaire auprès d'un cyber criminel, et débiter de petites sommes (ça passe inaperçu !) sur chacun de ces comptes usurpés !
Cette année, et à quelques mois d'intervalle, Orange, le premier opérateur en France a été piraté deux fois ! Le dernier vol de données concernait 1,3 million d'utilisateurs...

Imaginez le butin à disposition des malfrats ! Ne serait-ce qu'un débit de 49 euros sur chacun des comptes de ces 1,3 million de personnes... représenterait une somme de plus de 63 millions d'euros volés qui disparaitraient en quelques clics dans la nature !
Tous les prélèvements SEPA étant identifiés de la même façon sur votre relevé bancaire, un prélèvement de 49 euros n'attirerait peut-être même pas votre attention...

Un vrai jackpot pour les criminels !

Autre petit problème avec SEPA, puisque vous êtes le seul à pouvoir révoquer un prélèvement, si vous oubliez de le faire, vous ne pourrez vous en prendre qu'à vous-même. Normalement, un ordre de prélèvement était émis avec une durée d'engagement. Or maintenant, la banque n'a pas cette information.

Lorsque l'on sait que chaque français est prélevé en moyen par 4 à 5 créanciers chaque mois, un oubli est vite arrivé !
Avec SEPA, tant que vous ne signifiez pas clairement à un fournisseur que vous désirez révoquer son autorisation de prélèvement, celui-ci pourra en toute légalité continuer à se servir sur votre compte...

Déjà mis en place au Royaume-Uni, il y a de quoi faire des cauchemars...

Mis en place il y a quelques années au Royaume-Uni, ce système a de quoi trembler lorsque l'on regarde l'augmentation des prélèvements frauduleux...

Selon le *Center for Economics and Business research*, la hausse de ce type d'escroqueries atteindrait 30 % ! Selon l'UFC Que Choisir, au Royaume-Uni, où le mandat unique est utilisé depuis 10 ans, les fraudes par prélèvement sont passées de 1 % en 2000 à 10 % en 2010.

Pire en 2010, 26 000 personnes avaient été touchées par cette fraude, on en dénombrait près du double en 2013... Et les projections sont extrêmement sombres pour les années à venir

En France, les premières fraudes sont déjà en cours...

Plusieurs clients de différents établissements bancaires comme Boursorama Banque, Crédit Agricole, de BNP Paribas, ont reporté des prélèvements frauduleux sur leurs comptes en banque.

Depuis mai dernier, plusieurs dizaines de clients ont signalé des prélèvements suspects de 49,90 euros sur leur compte émis par une société dont ils n'avaient jamais sollicité les services et donc encore moins donné leur autorisation pour effectuer un prélèvement. Les témoignages de victimes peuvent d'ailleurs être consultés sur le forum du site cBanque.

« Cette petite mésaventure me fait m'interroger sur l'apparente facilité avec laquelle n'importe qui semble désormais pouvoir faire une demande de prélèvement sur un compte tiers sans l'autorisation de ce dernier.

Si certains dont je fais partie consultent très régulièrement leur compte, j'imagine que des personnes moins « à la page » [...] peuvent se voir réellement débitées sans s'en apercevoir... » écrit l'une des victimes de cette fraude.

La société émettrice de cette demande de prélèvement était cliente de ***La Banque Postale*** et a été rapidement repérée par la banque.

Les banques elles-mêmes s'attendent à une hausse exponentielle de ce type de fraudes, mais ne peuvent mettre en place que de toutes petites mesures de prévention...

Dans son guide, même le Comité national pour le SEPA avertit des dangers qu'encourent les usagers des banques en expliquant que : *« des risques réels de détournement existent pouvant mener à des mouvements de fonds non autorisés sur les comptes des débiteurs dont les identifiants ont été détournés. »*

Que faire en cas de fraude ?

Si vous veniez à repérer une tentative de fraude ou une fraude avérée sur votre compte, il n'y a pas de temps à perdre. Sachez que vous êtes en droit de demander le remboursement immédiat et intégral de la somme à votre banque en invoquant l'article L.133-18 du Code monétaire et financier.

Vous devez impérativement effectuer cette démarche **dans un délai de 13 mois après la date du prélèvement frauduleux** effectué sur votre compte.
Le problème d'après Serge Maître, Président de l'Afub (Association française des usagers des banques), c'est que les banques ont tendance à faire traîner le processus de remboursement.

Il conseille d'ailleurs *« Si une simple démarche à l'agence ne suffit pas à recréditer votre compte. Ses coordonnées figurent en général sur le relevé de compte. En règle générale, ces démarches suffisent à obtenir un remboursement ».*

La meilleure chose à faire est donc d'anticiper et de prendre des mesures pour éviter de vous faire prélever frauduleusement...

Votre stratégie Stop SEPA

REGLE NUMERO 1 :
Utilisez l'article 5.3d du règlement prévu par SEPA.

Cet article prévoit que **l'utilisateur peut établir une liste « blanche » de créanciers autorisés à prélever sur son compte en banque**.
Il peut également établir une liste « noire » énumérant les créanciers qui seront bloqués. Votre banque ne vous en parlera pas, mais vous avez cette possibilité donc n'hésitez pas à vous en servir !
Attention pensez absolument à mettre régulièrement cette liste sinon un créancier potentiel pourrait voir son prélèvement rejeté ce qui occasionnerait pour vous des frais bancaires.

REGLE NUMERO 2 :
Étudiez scrupuleusement votre relevé de compte.

Le moindre doute sur l'émetteur d'un prélèvement doit être regardé de près.
Contactez votre conseiller, et ne laissez pas traîner ces prélèvements. La prudence doit être de mise dès qu'un mouvement vous paraît suspect.

REGLE NUMERO 3 :
Surveillez les frais qui vous sont facturés par votre banque.

Comme le rappelait l'UFC Que Choisir, la hausse des tarifs bancaires est de plus en plus intenable, certains frais comme la simple tenue de compte ayant augmenté de 99 % en 4 ans seulement. Et avec l'arrivée de SEPA, vous pourriez bien découvrir de nouveaux frais spéciaux.
UFC Que choisir, révélait il y a quelques mois que 17 banques ont déjà mis en place des nouvelles facturations liées au SEPA, certaines continuent même de facturer des mises en place ou des révocations de prélèvements... alors même qu'elles ne gèrent plus ces opérations... Vigilance donc !
À chaque fois, interrogez votre banque et surtout demandez immédiatement le remboursement de ces frais... Mis bout à bout cela pourrait représenter de réelles économies pour vous. *Il ne faudrait pas qu'aux risques de se faire dépouiller par des criminels, vous vous fassiez piller par votre propre banque !*

Le Mot de la Fin

Un article des *Échos* sur les récentes prouesses de Bruxelles commençait par ces mots : *« Il fallait être aussi étourdis que nous le fûmes pour faire ce que nous fîmes »*. Je ne trouve pas de meilleure citation pour résumer tout ce que nous venons de voir ensemble. Des entités dans lesquelles nous avions d'habitude une confiance aveugle nous poussent aujourd'hui à redoubler d'attention pour combler leurs erreurs.

F Pourquoi avoir créé une carte bancaire ayant autant de failles ? Pourquoi l'imposer aux consommateurs ? Pourquoi ne pas prendre les mesures pour sécuriser la partie vulnérable de notre identité bancaire ?

Réponse : parce que cela couterait plus cher... parce que pour le moment il n'y a pas eu de fraude massive prouvée... parce que si l'on demandait aux gens, ils n'en voudraient pas...

Notre identité bancaire est sacrifiée sur l'autel des profits... Il y a de quoi être malade. Mais une attitude pareille des banques ne devrait pas nous surprendre au final.

Quant au système SEPA, ce laxisme, cette défaillance de la part de l'Europe est impardonnable. Ils savaient que cette réglementation faciliterait les fraudes, ils savaient que cette norme avait des failles béantes de sécurité, ils savaient qu'ils vous mettraient en danger... Alors pourquoi ?

Pour deux promesses qui se révèlent intenables... L'idée était belle, mais le résultat, comme souvent malheureusement, est à la fois décevant et dangereux. Dangereux, parce qu'au lieu d'unifier les pays sous une vraie économie connectée, cette réforme mal préparée risque d'exacerber la suspicion entre les états utilisant le SEPA.

Ces questions en appellent une autre, fondamentale :

Qu'il s'agisse de SEPA, du paiement sans contact ou du paiement via votre téléphone portable, **n'y a-t-il pas une volonté de réduire l'argent liquide au profit de l'argent électronique facilement traçable** ? Ne nous dirigerions pas vers un monde sans *cash* ?

Dans un certain sens, cela peut paraître logique. Après tout, quand l'argent physique aura disparu, tout ne sera plus qu'une question d'ordinateur, de monnaie virtuelle, d'argent numérique... et il sera bien plus facile de jouer à l'apprenti sorcier sur cette masse monétaire 2.0. Un clic pour réduire l'inflation, un pour réduire les déficits, un autre pour les dettes et un petit dernier pour prélever par-ci par-là sur des comptes dématérialisés de citoyen qui ne sera plus qu'un usager parmi d'autres de son propre compte bancaire.

Nous pensions que se faire voler sa carte bancaire sans que celle-ci ne sorte de notre poche relevait de la science-fiction...

Bienvenue à Hollywood !

Brochure de bienvenue J'agis ! La lettre de ceux qui choisissent leur vie

N° CPPAP : 0616 I 92354 – ISSN : 2274-4452 – Dépôt légal à parution – Publication mensuelle – Abonnement 1 an : 49 € TTC.

Directrice de la publication : Catherine Dourlens - Directrice de la rédaction : Lorraine Amiel - Maquette : Jean-Pierre Lecocq - Nos bureaux sont situés : 8, rue de la Michodière – CS50299 – 75081 Paris Cedex 02 – RCS Paris 399 671 809 – APE 5813Z.

Directrice de la publication : Catherine Dourlens – Directrice de la rédaction : Lorraine Amiel – Rédactrice en Chef : Anne Michel – Maquette : Stephan Nave.Nos bureaux sont situés : 8, rue de la Michodière – CS50299 – 75081 Paris Cedex 02 – RCS Paris 399 671 809 – APE 5813Z. – Service Clients : service-clients@paf-lifestyle.fr / La Rédaction : redaction@paf-lifestyle.fr – Impression : Imprimerie Delaroche, route de Villefranche, 12390 Rignac – Routage : Acti-média, 30 Bd Thibaud, 31100 Toulouse