La payement par Carte Bancaire sur Internet

Sommaire :

1) Préambule

Internet n'a jamais été, n'est pas et ne sera jamais 100% sécurisé. Malgré l'empilement des protections numériques, la source des problèmes de sécurité est et restera l'humain car on le retrouve à toutes les étapes d'un achat en ligne.

Cela commence par l'utilisateur et le peu de connaissance en sécurité informatique qu'il a acquis par lui-même, en entreprise ou via les médias populaires qui ne traitent que rarement ce sujet.
En plus de l'utilisateur, le problème peut également venir :

- de votre ordinateur infecté par un logiciel malveillant
- du magasin en ligne qu'il soit de bonne ou mauvaise réputation
- de votre banque ou d'un de ses prestataires de services

A toutes ces étapes, Il peut y avoir des personnes malhonnêtes, ou des employés mécontents. Il y aura toujours un hacker de génie ou à l'inverse un manque flagrant de sécurisation en un point de la chaîne.

Ce dossier traite uniquement du problème de l'utilisation de son numéro de carte bancaire lors d'achat en ligne et non pas des problèmes ou arnaques commerciaux qui n'ont pas attendu Internet pour exister.

2) Historique

Au début des années 2000 avec l'arrivé de l'ADSL et des boutiques virtuelles, les banques et les acteurs du secteur économique en ligne criaient haut et fort, mais à tort, que : *''tout était pour le mieux dans le meilleur des mondes virtuels 100% sécurisé''*. A l'époque, il ne fallait surtout pas inquiéter le consommateur pour ne pas tuer dans l'œuf cette nouvelle économie facteur de croissance.

Au cours de la décennie, les acteurs ont quand même dû changer leurs discours face à la multiplication des vols de numéro de carte bancaire via Internet. La médiatisation de ces vols et les rapports annuels de la Banque de France ont fortement contribué à ce changement. Quotidiennement à titre unitaire et quasiment mensuellement à grande échelle, la presse informatique spécialisée relate les problèmes de piratage de compte en ligne en tous genres et les numéros de carte bancaire n'échappent pas à cette triste réalité.

Malheureusement, même si le discours a changé et que l'on parle beaucoup plus de sécurité informatique comme la nécessité d'avoir un antivirus à jour, l'apparition des sites web sécurisés et le renforcement des contraintes d'indentification, dans les faits qui concernent l'achat en ligne par carte bancaire très peu de choses ont bougé.

3) Une situation actuelle anormale

Alors qu'il existe une vraie solution pour réduire très fortement les risques lors d'un achat en ligne, l'ensemble de ce secteur économique n'évolue pas et à ce jour, on dénombre seulement 6 établissements bancaires ayant mis en place le système facultatif et payant d'E-carte bleue (voir paragraphe 5).
Du coté des boutiques en ligne, on rechigne également à adopter le système 3D Secure qui décourage l'utilisateur lors de l'achat en ligne dans un pourcentage non acceptable par la boutique (voir paragraphe 4).

La cause de cet immobilisme vient du consommateur car son acte d'achat en ligne est freiné par les systèmes de sécurité mis en place. Pourtant, ce n'est pas le consommateur qu'il faut blâmer. Il est la victime d'un discours mensonger martelé depuis plus de dix ans par les acteurs économiques et les différents responsables politiques et économiques sur cette question du ''100% sécurité''.
De plus, du point de vue du consommateur, il est très simple et rapide de sortir sa carte bancaire et de saisir son numéro. Alors pourquoi faudrait-il maintenant changer ces habitudes pour un système plus long et plus compliqué? Surtout que le gouvernement a fait voter la loi de novembre 2001 protégeant le consommateur et obligeant la banque à rembourser son client victime de fraude.

Ne soyons pas dupe. Les banques ne sont pas des organismes philanthropes et les fraudes qui représentent 0,341 % en 2011 (voir le rapport annuel 2011 de la banque de France) sont mutualisées à l'ensemble des clients d'une banque en étant intégrées aux frais bancaires annuels. Bien sûr, ce coût est réactualisé chaque année en fonction de l'augmentation de la fraude. Ce pourcentage est faible mais exprimé en euros, il représente des centaines de millions.

L'image que renvoie cette loi est : *''Ne soyez pas responsable car de toutes façons, on vous rembourse !''*. Elle ne converge pas avec les récentes lois Hadopi qui rend pénalement responsable le titulaire d'une ligne ADSL qui doit sécuriser son accès Internet.

La mentalité des consommateurs doit évoluer comme cela a été le cas dans le domaine des assurances où un vol n'est pas remboursé s'il n'y a pas eu d'effraction. Ce fait est bien intégré dans l'opinion publique qui vous juge irresponsable si vous dites que vous ne fermez pas à clé votre véhicule ou votre habitation en partant.

N'attendons pas du gouvernement de faire voter une loi obligeant les banques à intégrer et à rendre obligatoire l'utilisation d'un service Ecarte bleue. Dans une période économique difficile pour ne pas dire en crise, il ne faut pas prendre le risque de perdre quelque centièmes ou millièmes de points de croissance.
N'attendons pas non plus qu'une entité de régulation d'Internet oblige les sites de vente en ligne à systématiser 3D Secure.
Tant que le pourcentage de fraudes est acceptable, c'est-à-dire qu'il peut être inclus dans les frais bancaires sans provoquer la grogne du consommateur, il n'y aura pas de grand changement.

4) 3D Secure

Définition

Ce protocole de paiement en ligne a été développé par Visa et Mastercard et consiste à s'assurer, lors de chaque paiement en ligne, que la carte est bien utilisée par son titulaire.

Dans ce cas où, à la fois le commerçant et la banque du porteur de la carte sont équipés, une étape supplémentaire a lieu au moment du paiement. En plus du numéro de carte bancaire, de la date d'expiration de la carte et des trois chiffres du code de sécurité (imprimés au dos de la carte), l'internaute doit saisir un mot de passe, tel que sa date de naissance (authentification simple) ou un code dynamique à usage unique (authentification forte).

Pour plus de détails vous pouvez lire le dossier du site commentcamarche.net à ce sujet :
http://www.commentcamarche.net/faq/16311-3d-secure-verified-by-visa-securecode-qu-est-ce-que-c-est

Problèmes (sources wikipédia)

- 3D Secure ne résout en rien le problème de fond car lors de l'achat, vous avez saisi votre vrai numéro de carte bancaire, la date d'expiration et le cryptogramme visuel. Si ces informations sont interceptées, elles peuvent être utilisées sur des sites n'étant pas 3D Secure ou pour créer une carte réelle à utiliser dans tout endroit ne demandant pas la saisie du code confidentiel de la carte.
- Ce système est juste bon pour limiter la fraude pour les magasins en ligne qui le pratiquent.
- Si vous êtes victimes de fraude sur une transaction 3D Secure, vous allez être en porte à faux vis-à-vis de votre banque.
- Le label « Vérifié par Visa » a été l'objet de critiques parce qu'il est difficile de faire la différence entre un pop-up authentique et celui qui aurait été généré par un site frauduleux. En effet le pop-up provient d'un domaine qui n'est pas forcément celui du site où a été fait l'achat, ni celui de la banque d'où provient la carte, et pas non plus celui de visa.com. Du fait, le système « Vérifié par Visa » a été lui-même la cible de phishing.
- J'espère que la validation 3D Secure ne se fait plus avec la date de naissance, car le risque de fraude reste fort. Grâce aux nombreux réseaux sociaux (de type Facebook par exemple), il est très facile d'obtenir la date de naissance d'un internaute et donc contourner cette protection.
- Une transaction 3D Secure ne doit jamais être modifiée, dès que le commerçant fait du débit partiel ou une duplication de la demande pour un débit supérieur, la protection 3D Secure n'est plus garantie.

5) L'E-carte bleu

Définition

Pour chaque transaction, votre banque vous fournit un numéro de carte bancaire unique, valide sur une courte période, pour un seul achat et un montant maximum. A l'heure actuelle, c'est à mon sens la méthode présentant le plus de sécurité.

Utilisation

Ce service est disponible soit sur le site Internet de la banque soit via un logiciel à installer sur votre ordinateur.
Lors d'un achat en ligne quand vous avez le montant total de la commande avec la TVA et les frais de ports inclus :

- Vous lancez le logiciel E-carte bleue fourni par votre banque (ou vous vous connectez au site de votre banque).
- Vous saisissez l'identifiant et le mot de passe associé à ce service E-carte bleue
- Vous entrez le montant total de votre commande
- Le logiciel vous indique un numéro de carte bleu, un cryptogramme visuel et une date de validité. Le tout étant différent des informations de votre vraie carte bancaire.
- Vous n'avez plus qu'à saisir ces informations dans la page payement et valider votre achat.
- Une foi l'habitude prise, l'obtention du numéro prend 1 minute à 30 secondes.

Retour au Sommaire

Les avantages

- Vous ne saisissez jamais votre vrai numéro de carte bleu, vrai date d'expiration et vrai cryptogramme visuel.
- Même si les informations du numéro unique de l'E-carte bleue sont interceptées, elles ne seront utilisables que pour une transaction et pour le montant maximum que vous avez indiqué. De plus, il faudrait que le pirate fasse un achat avant vous. Comme vous validez votre achat dans les dizaines de secondes qui suivent l'obtention du numéro, le risque est quasi nul même si la fraude est techniquement réalisable.
- Comme vous vous rendez sur le site de votre banque ou via le logiciel, le phising par popup frauduleux est éliminé.

Les risques

- Votre identifiant et votre mot de passe pour ce service restent le maillon faible. Ils ne doivent être connu que de vous et stockés dans un lieu sûr sur papier ou crypter dans un document numérique.
- On pourrait imaginer qu'un hacker installe un faux logiciel E-carte bleue sur votre ordinateur permettant la récupération de votre identifiant et mot de passe du service.

Listes des banques utilisant ce service

Ce service et facultatif et payant. Reportez-vous aux conditions propres à chaque banque pour ce service.

Etablissement bancaire	Lien vers le service E-carte bleu
La banque Postale	E-Carte Bleue
LCL	E-Carte Bleue
Société Générale	E-Carte Bleue
La Banque Populaire	E-Carte Bleue
Caisse d'Epargne	E-carte Bleue

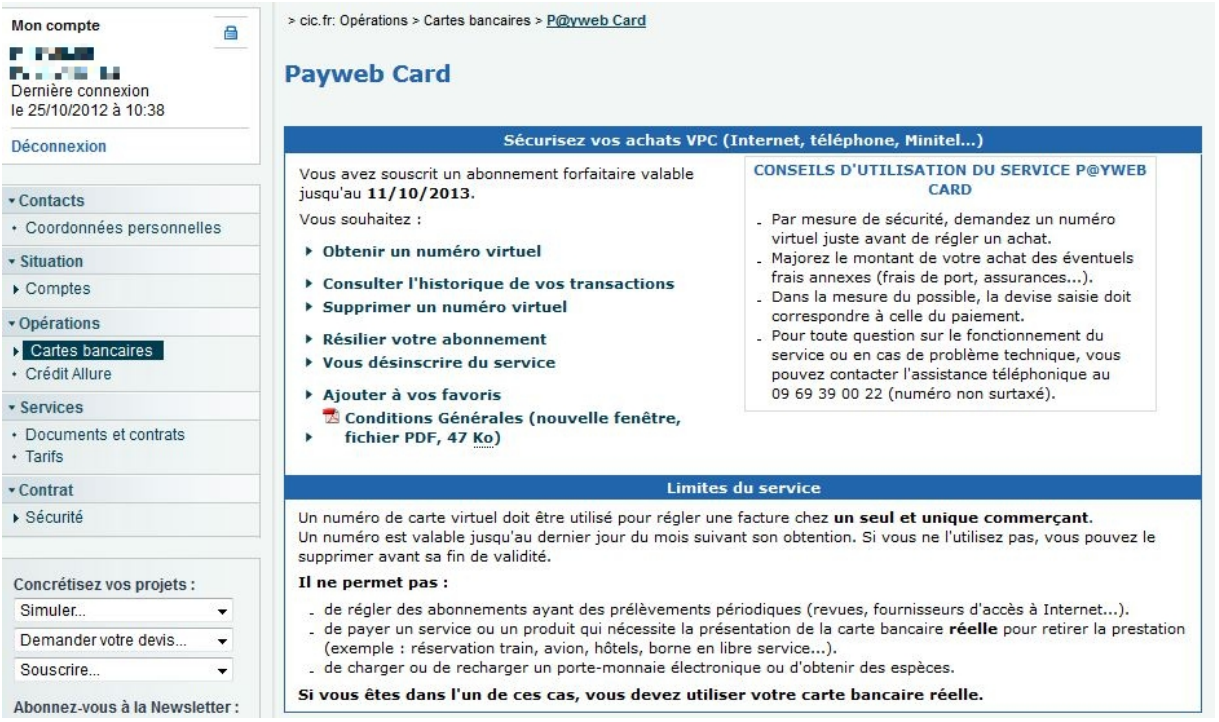
Le cas du CIC : la meilleure protection existante

Etablissement bancaire	Lien vers le service E-carte bleu
CIC	Payweb Card

Le CIC est à montrer en exemple car il propose une solution E-carte bleue renforcée avec plusieurs niveaux d'identification. Une foi l'habitude prise, l'obtention du numéro prend 1 à 2 minutes.

Vous vous rendez sur le site du CIC (ou sur le logiciel CIC installé sur votre ordinateur et vous saisissez l'identifiant et le mot de passe de votre compte en ligne).

Dans la section Opérations\Cartes bancaires\P@yweb Card, cliquez sur ''Obtenir un numéro virtuel''.



A cette étape vous devez saisir, la clé de 4 chiffres correspondant à la case demandée.

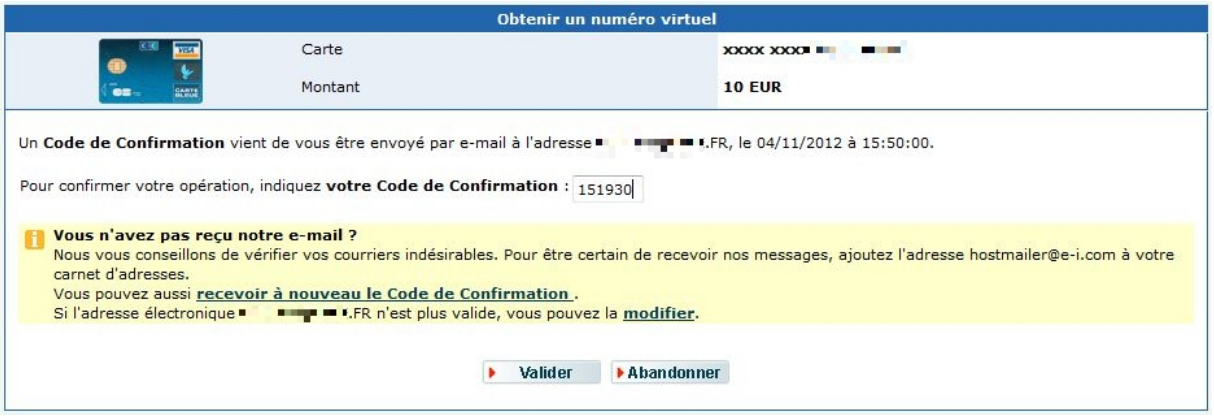
Cette case se trouve sur la Carte de Clés Personnelles qui vous a été remis par lettre recommandée après l'inscription à ce service.

Retour au Sommaire

Dans l'étape suivante, vous indiquez le montant de la transaction

Lors de l'inscription à ce service vous avez indiqué une adresse email de contact et vous recevez un email avec un code de confirmation à 6 chiffres qui expire dans un délai court de 15 min.

Vous inscrivez ce code de confirmation dans la zone prévu à cet effet et vous validez.



Vous obtenez votre numéro unique et vous pouvez copier/coller les informations pour

Retour au Sommaire

.

Restriction d'utilisation de l'E-carte bleue

Ce service ne permet pas :

- de régler des abonnements ayant des prélèvements périodiques (revues, fournisseurs d'accès à Internet...).
- de payer un service ou un produit qui nécessite la présentation de la carte bancaire réelle pour retirer la prestation (exemple : réservation train, avion, hôtels, borne en libre-service...).
- de charger ou de recharger un porte-monnaie électronique ou d'obtenir des espèces.
- Si vous êtes dans l'un de ces cas, vous devez utiliser votre carte bancaire réelle.

D'une manière générale, les services et produits nécessitant la présentation de la carte bancaire réelle sont de réels problèmes de sécurité.
Le cryptage et la protection des serveurs des hôtels sont souvent pointés du doigt. En ce qui concerne des billets de train ou d'avion, je m'étonne fortement de ce procédé car une carte bancaire n'est pas une pièce d'identité.

Retour au Sommaire

6) Conclusion

Mais pourquoi donc perdre du temps à obtenir un numéro unique lors d'un achat en ligne et en plus payer ce service?

Outre le fait (mentionné en début de dossier) d'être responsable, la perte de temps à chaque achat n'est rien à comparer des démarches administratives à faire lors du vol de votre vrai numéro de carte bancaire.

- Faire l'annulation de votre carte bancaire
- Demander et attendre votre nouvelle carte
- Lister les débits frauduleux sur vos relevés de compte
- Se rendre au commissariat ou au poste de police de votre domicile pour déposer plainte et passer facilement 2 heures voir ½ journée en cas d'attente.
- Ecrire une lettre manuscrite à votre banque accompagnée de votre procès-verbal
- Attendre de très longs mois que le remboursement soit effectué sur votre compte bancaire.

Au pire des cas, on peut également ajouter le risque d'avoir d'importants problèmes bancaires liés aux découverts imprévus et l'émission de chèques pendant cette période.

Oui, vous pouvez faire des achats en ligne mais pas avec votre véritable numéro de carte bancaire. Il faut utiliser un numéro unique virtuel via E-carte bleue.

Si votre banque ne propose pas ce service E-carte bleue, il y a toujours la possibilité de régler par virement bancaire ou par chèque.
Enfin, si avez décidez de changer d'établissement bancaire, l'option E-carte bleue est un plus à prendre en compte dans les choix à votre disposition.

L'avenir

La fusion entre sécurité et facilité d'utilisation est peut d'être dans la nouvelle carte présentée par MasterCard en novembre 2012.

Cette carte intègre un petit écran LCD, un clavier numérique tactile et un bouton d'allumage. Entre autre chose, l'utilisateur peut générer une clé unique et temporaire à utiliser pour valider une transaction en ligne. Il faudra utiliser le clavier pour taper un code de protection, qui permettra ensuite d'accéder à la clé sur l'écran LCD.

Retour au Sommaire