

Les cybercriminels ciblent le paiement mobile | Le Net Expert Informatique



Les cybercriminels
ciblent le paiement
mobile

Il y a quelques semaines, nous avons traité, du e-Commerce. C'est un registre si vaste et varié que nous choisissons, cette semaine aussi, d'y consacrer quelques réflexions, histoire de susciter chez nos lecteurs quelque intérêt pour une problématique appelée à devenir incontournable. Malgré l'essor du e-Commerce, les modes de paiement mobile peinent à décoller dans de nombreux pays développés. En cause, le conservatisme et la peur de l'inconnu.

L'inconnu, selon de nombreux spécialistes, c'est la cybercriminalité qui donne des sueurs froides aux fournisseurs de solutions. Dans un excellent article au titre très évocateur publié récemment, « Le paiement mobile, nouvel eldorado des escrocs », Benoît Huet de la rédaction de lemondeinformatique.fr nous amène faire une immersion dans les méandres d'un secteur pourtant promu à un bel essor. Les résultats du paiement mobile, il faut bien le concéder, sont assez modestes.

Dans son article, Benoît Huet écrit : « Selon l'institut d'études GFK, qui a mené une enquête dans 17 pays auprès de 17 000 consommateurs, seulement 5% des transactions mondiales sont réellement effectuées avec un appareil mobile ». Presqu'un désert ! Dans un pays comme la France, notre référence à tous, « les transactions via le paiement mobile sont souvent estimées à moins de 1% par les différents cabinets d'études ».

Et pourtant, précise l'article de notre confrère, ce n'est pas faute d'avoir essayé. De nombreuses applications permettant de payer avec un smartphone existent : le service PayByPhone pour payer le stationnement et le parking à Boulogne, Nice et dans d'autres villes, ainsi que des commerces qui ont mis en place un terminal NFC (Paiement Sans Contact) pour régler diverses courses.

La première raison, et nous l'évoquons plus haut, le conservatisme culturel : « Si le paiement mobile a encore du mal à percer en France, c'est déjà parce que les moyens de paiement sont très liés à la culture des pays. La France est par exemple un pays fortement tourné vers l'usage de la carte bleue Visa alors qu'en Belgique, c'est la Mastercard qui règne, quant à l'Allemagne, le paiement en liquide est encore très courant ».

Sans vouloir défier la technologie, « Les français ne sont pas encore prêts à payer avec leur mobile, c'est à la fois un problème culturel et un manque de confiance dans les technologies, ils préfèrent donc payer en caisse avec une carte, de l'espèce ou en chèque ».

La seconde raison qui plombe l'essor du paiement mobile vient d'être lâchée : le manque de confiance dans les technologies. Par instinct de survie, la majorité des français boudent le paiement mobile, moins sécurisé à leurs yeux, de peur d'être victime des cyberescrocs qui ont plus d'un tour dans leur sac.

Sans l'affirmer, les conclusions de l'étude donnent raison aux cyber-sceptiques qui semblent se perdre dans la jungle des technologies de communication sans contact comme les balises (Beacons utilisant le Bluetooth) ; le RFID ; le NFC (qu'utilise Apple, entre autres, avec Apple Pay et Google avec Google Wallet) ; le QR code (comme le Flash'NPay créé par Auchan) ; la transmission magnétique (Samsung Pay exploite la technologie transmission magnétique suite au rachat de LoopPay mais aussi le NFC) ; les systèmes de portefeuilles électroniques mobiles comme Orange Cash (Orange et Visa) ; PayPal Mobile et Paylib (initié par les banques françaises). Jungle, il faut bien l'admettre, est vraiment un doux euphémisme pour évoquer cet univers ! Face à un tel environnement, banques et entreprises n'ont d'autres choix que de perfectionner la sécurité des systèmes de paiement mobiles afin de donner davantage d'assurance aux consommateurs.

Cette assurance semble passer par des systèmes de cryptage des données très évolués et les dispositifs de détection prédictive de malwares. Notre confrère cite PayPal qui vient de racheter la start-up israélienne CyActive qui a mis au point une technologie capable d'anticiper les futures attaques grâce à des algorithmes permettant d'analyser et de comprendre les processus de piratage.

En parallèle, les fournisseurs ne ménagent pas leurs efforts en apportant, au niveau du terminal, des mécanismes à double authentification comme Apple qui exploite l'empreinte digitale en plus d'un code de sécurité unique et des quatre derniers numéros de la carte de sécurité sociale de l'utilisateur. On le voit bien, il y a de gros efforts en cours pour tendre vers le risque zéro, même s'il n'existe pas.

Les entreprises du secteur et les banques gagneraient à collaborer plus étroitement pour améliorer la sécurité des transactions au plan national et international, tout comme elles sont condamnées à imaginer des standards qui détectent à mille lieues les criminels et les neutralisent sans coup férir.

Enfin, chaque entreprise qui propose des solutions de paiement mobile devrait assortir son plan d'expansion d'une campagne de communication qui permettrait aux utilisateurs d'éviter de tomber dans les pièges, de plus en plus perfectionnés, des cybercriminels.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.

Contactez-nous

Cet article vous plaît ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://malijet.com/la_societe_malienne_aujourd'hui/139922-chronique-du-web-les-cybercriminels-ciblent-le-paiement-mobile.html
Par Serge de MERIDIO