Denis JACOPINI sur LCI : Les techniques des cybercriminels pour pirater votre CB

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
					

Denis JACOPINI sur LCI : Les techniques des cybercriminels pour pirater votre CB

Denis Jacopini, expert informatique assermenté spécialisé en cybercriminalité, explique que quoi que l'on fasse, les fraudeurs auront une longueur d'avance. Néanmoins, il y a des failles dans le système, et en particulier au niveau du cryptogramme visuel.

En direct sur LCI avec Serge Maître Maître, président de l'AFUB (Association Française des Usagers des Banques) et Nicolas CHATILLON, Directeur du développement-fonctions transverses du groupe BPCE et Denis JACOPINI, Expert informatique assermenté spécialisé en cybercriminalité débattent le 7 mars 2016 sur les techniques des cybercriminels pour vous pirater votre CB.


http://lci.tf1.fr/france/societe/cartes-bancaires-les-fraudeurs-ont-toujours-une-longueur-d-avance-8722056.html

Une liste non exhaustive avec 10 techniques de cybercriminels pour vous pirater votre carte bancaire : http://www.lenetexpert.fr/10-techniques-de-cybercriminels-pour-vous-pirater-votre-carte-bancaire/

Réagissez à cet article

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220

Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.
Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.
Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?
Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.
Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !
Commandez sur Fnac.fr

---

https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la

Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : *Cartes bancaires : « Les fraudeurs ont toujours une longueur d'avance » – Société – MYTF1News*

Pouvez-vous refuser la carte sans contact délivrée par votre banque ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Pouvez-vous refuser la carte sans contact délivrée par votre banque ?				

La Cnil rappelle que les banques doivent informer leurs clients que leur carte bancaire dispose de la fonction paiement sans contact, une option que ces derniers sont libres de refuser.

En France, plus de 33 millions de cartes de paiement ont des fonctionnalités sans contact, ce qui représente plus de 50 % des cartes en circulation, rappelle la Cnil (Commission nationale de l'informatique des libertés). Grâce à ce système, il est possible d'utiliser sa carte bancaire sans avoir à taper son code secret lorsque les achats sont inférieurs à 20 euros. Depuis la recommandation de la Cnil de juillet 2013, les porteurs de ce type de carte doivent être clairement informés de la fonctionnalité sans contact et doivent pouvoir la refuser.

Comment exercer son droit d'opposition ?
Dans un premier temps, le client doit se tourner vers sa banque pour lui demander la désactivation ou la réédition gratuite d'une nouvelle carte dépourvue de la fonctionnalité paiement sans contact.
Les banques sont libres de choisir les moyens à engager pour respecter ce droit d'opposition. Certaines proposent de distribuer une nouvelle carte identique aux anciens modèles, d'autres incitent à une désactivation via le site internet de la banque.
Si la banque ne respecte pas son devoir d'information ou si elle refuse de désactiver le paiement sans contact, le client peut alors s'adresser au service des plaintes de la Cnil, sur le site internet de la Commision, en appelant le 01 53 73 22 22 (du lundi au vendredi de 10h à 12h et de 14h à 16h) ou en écrivant un courrier à la Cnil – Service des plaintes – 8, rue Vivienne – CS 30223- 75083 Paris cedex 02

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en*

conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :

Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Denis JACOPINi en direct sur LCI : « Les fraudeurs ont toujours une longueur d’avance – MYTF1News | Denis JACOPINI

	Denis JACOPINi en direct sur LCI : « Les fraudeurs ont toujours une longueur d’avance – MYTF1News

Denis Jacopini, expert informatique assermenté spécialisé en cybercriminalité, explique que quoi que l'on fasse, les fraudeurs auront une longueur d'avance. Néanmoins, il y a des failles dans le système, et en particulier au niveau du cryptogramme visuel.

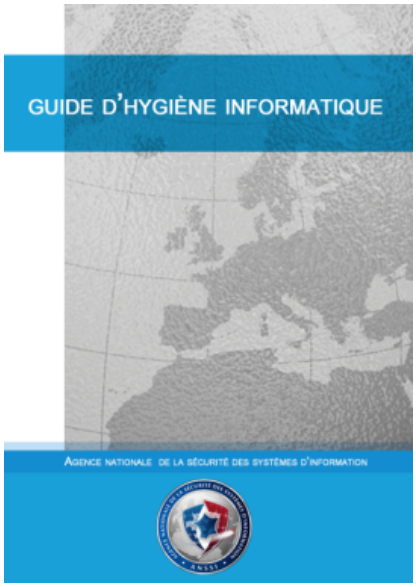
En direct sur LCI avec Serge Maître Maître, président de l'AFUB (Association Française des Usagers des Banques) et Nicolas CHATILLON, Directeur du développement-fonctions transverses du groupe BPCE et Denis JACOPINI, Expert informatique assermenté spécialisé en cybercriminalité débattent sur les techniques des cybercriminels pour vous pirater votre CB.


http://lci.tf1.fr/france/societe/cartes-bancaires-les-fraudeurs-ont-toujours-une-longueur-d-avance-8722056.html

Réagissez à cet article

Source : *Cartes bancaires : « Les fraudeurs ont toujours une longueur d'avance » – Société – MYTF1News*

Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique | Denis JACOPINI



Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique

Vous voulez éviter que le parc informatique soit utilisé pour affaiblir votre organisation ? L'un des guides publiés par l'ANSSI vous aidera à vous protéger.

Initialement destinés aux professionnels de la sécurité informatique, les guides et recommandations de l'ANSSI constituent des bases méthodologiques utiles à tous. Vous trouverez sans peine votre chemin en utilisant les mots-clés, qu'un glossaire vous permet d'affiner, ou le menu thématique.

LISTE DES GUIDES DISPONIBLES

- Guide pour une formation sur la cybersécurité des systèmes industriels
- Profils de protection pour les systèmes industriels
- Sécuriser l'administration des systèmes d'information
- Achat de produits de sécurité et de services de confiance qualifiés dans le cadre du rgs
- Recommandations pour le déploiement sécurisé du navigateur mozilla firefox sous windows
- Cryptographie – les règles du rgs
- Recommandations de sécurité concernant l'analyse des flux https
- Partir en mission avec son téléphone sa tablette ou son ordinateur portable
- Recommandations de sécurité relatives à active directory
- Recommandations pour le déploiement sécurisé du navigateur microsoft internet explorer
- l'homologation de sécurité en neuf étapes simples,
- bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,
- recommandations pour le déploiement sécurisé du navigateur google chrome sous windows,
- usage sécurisé d'(open)ssh,
- la cybersécurité des systèmes industriels,
- sécuriser une architecture de téléphonie sur ip,
- mettre en œuvre une politique de restrictions logicielles sous windows,
- prérequis à la mise en œuvre d'un système de journalisation,
- vulnérabilités 0-day, prévention et bonnes pratiques,
- le guide des bonnes pratiques de configuration de bgp,
- sécuriser son ordiphone,
- sécuriser un site web,
- sécuriser un environnement d'exécution java sous windows,
- définition d'une politique de pare-feu,
- sécuriser les accès wi-fi,
- sécuriser vos dispositifs de vidéoprotection,
- guide d'hygiène informatique,
- la sécurité des technologies sans contact pour le contrôle des accès physiques,
- recommandations de sécurité relatives à ipsec,
- la télé-assistance sécurisée,
- sécurité des systèmes de virtualisation,
- sécurité des mots de passe,
- définition d'une architecture de passerelle d'interconnexion sécurisée,
- ebios – expression des besoins et identification des objectifs de sécurité,
- la défense en profondeur appliquée aux systèmes d'information,
- externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques,
- archivage électronique… comment le sécuriser ?
- pssi – guide d'élaboration de politiques de sécurité des systèmes d'information,
- tdbssi – guide d'élaboration de tableaux de bord de sécurité des systèmes d'information,
- guide relatif à la maturité ssi,
- gissip – guide d'intégration de la sécurité des systèmes d'information dans les projets

---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/

Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits | Denis JACOPINI

Ce sont les vacances mais nombre de touristes ne se séparent pas de leurs smartphones, tablettes ou ordinateurs portables. Et pour se connecter à l'internet, quoi de mieux qu'attraper un wi-fi gratuit. Une pratique qui peut se révéler très dangereuse. Des proies faciles pour les « sniffeurs » de données. Explications de Laurent Heslault, expert sécurité chez Symantec.

Vous êtes sur votre lieu de vacances et vous avez envie de vous connecter à l'internet. Pour consulter votre messagerie ou vos réseaux sociaux, envoyer des photos à vos proches, surfer sur le net ou consulter votre compte en banque ou faire une réservation.
Solution la plus simple : se connecter à un réseau Wi-Fi gratuit. Dans votre hôtel, camping, à la terrasse d'un café ou d'un restaurant… Les accès gratuits pullulent et se généralisent.
Expert en sécurité à Symantec, Laurent Heslault tire le signal d'alarme. « **Rien de plus simple que de pirater les données qui transitent sur un réseau Wi-Fi gratuit** » assure-t-il. « **Par exemple, je m'installe à la terrasse d'un café et je crée un vrai faux point d'accès gratuit en empruntant le nom du café. Des gens vont s'y connecter et je n'ai plus qu'à récupérer toutes les données qui m'intéressent. Des mots de passe, des identifiants…** »

Des sniffeurs de données

Il exagère ? Non. « **L'expérience a été faite à la terrasse d'un café. Nous avons installé un logiciel qui permet de sniffer tous les appareils qui se branchaient sur le Wi-Fi. Ensuite, des complices, qui se faisaient passer pour des magiciens, allaient voir les gens en disant que par magie, ils avaient réussi à changer le code de leur téléphone ou leur image sur Facebook. Ils étaient étonnés** ! » Rien de magique mais des logiciels de piratage qui se trouvent facilement sur le net.

Les données sur le Wi-Fi ne sont pas chiffrées

« **Les données qui transitent sur le Wi-Fi ne sont pas chiffrées. Sauf quand vous vous connectés à un site sécurisé avec le protocole HTTPS. Donc ce sont des données faciles à intercepter.** » Danger sur les vrais faux points d'accès Wi-Fi mais aussi sur les vrais qui ne sont, dans la grande majorité des cas, pas chiffrés non plus. « **Par contre pas de problème pour une connexion 3G ou 4G qui sont chiffrées. Mais pour économiser leur forfait, les gens préfèrent se connecter au Wi-Fi** ».

Conseils

Alors quels conseils ? « **Ne jamais, sur un Wi-Fi public, entrer un mot de passe. D'autant que la plupart des internautes utilisent le même mot de passe pour tous leurs sites.** » En clair, limiter les dégâts en ne consultant que des sites qui ne demandent aucune identification.
Autre solution : protéger son smartphone ou sa tablette en y installent un logiciel qui va chiffrer toutes les données qui vont en sortir. Plusieurs types de logiciels existent dont le Wi-Fi Privacy de Norton qui est gratuit pendant 7 jours et peut s'installer sur des périphériques fonctionnant sous Ios et Androïd.
Article original de Samuel NOHRA.

Nous prodiguons une multitude d'autres conseils durant les formations que nous animons à destination des élus, chef d'entreprises, agents publics et salariés. [Consultez la liste de nos formations]

Réagissez à cet article

Original de l'article mis en page : Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

---

Une puce RFID sous la peau. Des salariés volontaires

l’ont essayé…

	Une puce RFID sous la peau. Des salariés volontaires l’ont essayé…

Une entreprise belge a implanté une puce RFID sous la peau de huit de ses salariés volontaires. Rencontre.

Accepteriez-vous de vous faire pucer pour le boulot ?
C'est ce qu'ont consenti huit des douze salariés d'une agence digitale belge, comme avant eux une entreprise suédoise : mi-décembre, au milieu de leur petit open space blanc et rouge, un pierceur néerlandais leur a logé sous la peau, entre la base du pouce et l'index, une puce RFID (radio frequency identification).
L'une de celles que l'on implante habituellement sous le poil des animaux de compagnie ou des brebis.
Sa silhouette sombre, longue comme un grain de riz, apparaît à travers la chair quand l'un des salariés pucés serre le poing pour nous la montrer.
Comme il l'a fait devant d'autres journalistes avant nous, Tim Pauwels se plie allègrement à la démonstration : sur le trottoir de Malines, ville grise entre Bruxelles et Anvers où l'entreprise est située, il colle avec délicatesse sa main sous l'interphone. Bip!
Miracle tant attendu : la porte s'ouvre. Nous entrons.

« Adoptons la technologie »

L'idée de se faire implanter une puce pour ouvrir la porte de leur boîte leur est venue un vendredi. A l'instar des si cool entreprises de la Silicon Valley, les salariés de Newfusion ont chaque semaine « deux heures de libre » dédiées à la cogitation de projets.
Parce que certains oubliaient régulièrement leur clé, ils ont lancé un vendredi le projet de les remplacer par un système électronique de badges. « Plus facile, plus digital », précise dans un anglais fluide Vincent Nys, 27 ans, qui a lancé NewFusion il y a quatre ans.
« On a passé deux jours dessus, on l'a mis en place mais quelques jours plus tard, ils oubliaient leur carte. Alors on a réfléchi : « quelle est la prochaine étape ? » Nous voulions faire quelque chose d'innovant et ouvrir une discussion. »

Une puce RFID et l'un des kits commandés par Newfusion (Emilie Brouze)
En parfaite adéquation avec son époque, Vincent Nys adore l'innovation (il répète le mot à l'envi). Les milliers de personnes dans le monde qui possèdent une puce électronique se divisent à son sens en deux catégories. Ceux qui le font pour se différencier – « être unique, spécial » – et les consommateurs précoces, « comme nous ». Ceux qui n'ont pas peur de se dire :

« Adoptons la technologie et allons plus loin. »
Son associé complète :
« Ceux qui avancent sont ceux qui ouvrent les portes aux autres… Il faut innover pour pouvoir faire des progrès. »
Innovons donc en ouvrant des portes.

« Est-ce qu'on le sent ? »

Avant de commander les puces à une entreprise américaine qui les commercialise en kits stérilisés, il y a tout de même eu discussion au sein de Newfusion. « On a eu un débat, mais pas celui qu'il y a dans les médias », rétorque Vincent Nys :
« Est-ce que c'est sûr ? Est-ce qu'il y a des implications médicales ? Est-ce qu'on pourra passer un scanner ? Est-ce qu'on le sent ? Est-ce que ça à un impact sur notre vie ? »
Seulement quatre salariés ont refusé de se faire pucer. « Je ne perds pas mon badge, je n'ai pas vu l'intérêt d'une puce », répond Sam Van Campenhout, développeur.
« Je crois que je n'aimerais pas avoir quelque chose sous ma peau. C'est bizarre », ajoute Sil Colson, jeune designer multimédia.

Sil Colson fait partie des salariés ayant refusé de s'implanter une puce RFID (Emilie Brouze)

Ce qui pourrait la faire changer d'avis ? Que la puce contienne son passeport et qu'il suffise de présenter sa main au moment des contrôles, sans risquer d'oublier ou d'égarer le document en vacances. Ou que la puce contienne les infos essentielles de son carnet médical, immédiatement accessible en cas d'urgence. Pour ouvrir la porte d'entrée, Sil préfère conserver son badge.
Un autre développeur raconte que lui a tout de suite été enthousiaste à l'idée (sa copine un peu moins) : « J'adore la technologie. »
En quelques heures, il a bidouillé un programme que le patron lui demande de nous montrer. Alors Dries Van Craen presse sa main droite contre un boîtier relié à son ordinateur. Bip! (La sonorité est la même qu'à la caisse d'un supermarché.)
S'affiche sur l'écran, sur un fond automnal, un message de bienvenue personnalisé. Sur la colonne de droite sont empilés ses morceaux de musique préférés, au-dessus des temps de transport pour rentrer chez lui, actualisés en temps réel.
Le patron s'enthousiasme :
« Voilà ce que tu peux faire sans argent et en une demi-journée. Avec des années et une vision, on pourra faire plein de choses. »
Le jeune patron technophile a installé chez lui un système lui permettant d'ouvrir la porte de son domicile d'un geste de la main.
Prochaine étape : bricoler un moyen de régler son éclairage intérieur grâce à la même puce (un jeu de lumières pour ses soirées en solitaire, un autre quand il est avec sa compagne).

« Disrupter » le marché

Quand on lui fait remarquer l'utilité à ce stade toute relative de ces puces sous-cutanées, Vincent Nys assume. Parce qu'il ne s'agit pas que de se débarrasser des badges d'entrée : c'est une piste de développement pour Newfusion.
« Dans nos têtes, on ne s'est même pas demandé ce qu'on pouvait faire avec [les puces RFID]. On s'est dit « Allons-y, faisons-le ». On ne s'est pas trop préoccupé de questions éthiques, morales et des possibles applications.
On pense qu'il faut être les premiers à le faire. On commence par « disrupter » le marché, puis on créé des applications. «
Sur la RTBF, qui a diffusé l'un des premiers reportages sur l'opération de puçage, Alexis Deswaef, président de la ligue des Droits de l'Homme en Belgique, soulevait une question éthique : « Dans le futur, braderons-nous un peu plus nos droits à la vie privée pour plus de sécurité ou de confort ? »
En dépit des critiques, Vincent Nys, comme son associé, sont ravis des retombées médiatiques, eux qui espéraient intéresser seulement quelques blogs techs avec leur communiqué de presse : on parle d'eux dans le monde entier. Quelle bonne pub ! Des banques, une société de transports publics ou encore une municipalité ont d'ores et déjà pris contact avec eux.

« Big Brother »

A côté de ces potentiels nouveaux clients, Newfusion a aussi reçu une cinquantaine de messages désagréables. « Des gens qui faisaient référence aux années Hitler – parce qu'on marquait les gens -, des personnes qui nous traitaient d'antéchrist ou nous parlent de Big Brother… » Beaucoup d'après lui n'ont pas bien compris la technologie.
Vincent Nys fait défiler certains commentaires Facebook sur son téléphone : « Ce n'est pas éthique », « 0% liberté », « il est temps que je lise de nouveau « 1984 » »… Il remarque :
« Ils sont tous fixés sur ce livre. »

Vincent Nys, fondateur et directeur de Newfusion, le 9 février 2017 à Malines (Emilie Brouze)
Au début, le patron répondait poliment et pédagogiquement à ceux qui ne sont manifestement pas mûrs pour "aller plus loin" : non, non, non, il ne s'agit pas de traquer les gens. La puce RFID qu'il a lui aussi sous la peau fonctionne sans batterie et ne peut pas transmettre à un tiers la localisation du porteur.
Elle contient un numéro unique ainsi qu'un espace mémoire lui permettant par exemple d'enregistrer sa carte de visite pour la donner à un client en posant sa main sur son smartphone.
Alors oui, le patron peut savoir exactement quand un des employés pucés entre ou sort du bâtiment, « comme avec les badges ou la caméra fixée à l'extérieur », semble-t-il relativiser. « Mais ce n'est pas le but et ce n'est pas notre culture. Les employés ont des horaires de travail souples. »…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Travailleurs belges pucés : « On ne s’est pas trop préoccupé de questions éthiques » – L’Obs

---

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'évoquions 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.

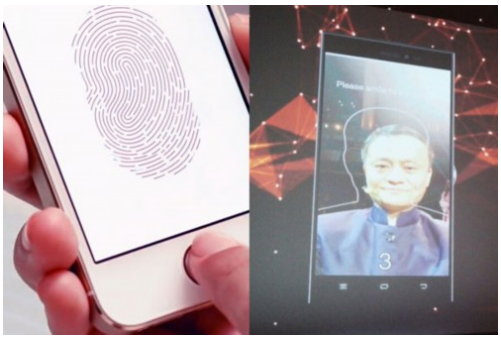
Les entreprises du secteur et les banques gagneraient à collaborer plus étroitement pour améliorer la sécurité des transactions au plan national et international, tout comme elles sont condamnées à imaginer des standards qui détectent à mille lieues les criminel et les neutralisent sans coup férir.

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

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

Alibaba va lancer un service de paiement facial mobile plus sûr | Le Net Expert Informatique

	Alibaba va lancer un service de paiement facial mobile plus sûr

Selon une nouvelle publiée le 16 mars par la chaine d'informations financières américaine CNBC, le géant du commerce électronique chinois Alibaba développe actuellement une technologie de « paiement facial », qui permettra l'authentification de l'identité de l'utilisateur grâce à son smartphone qui scannera le visage de celui-ci, ce qui permettra d'assurer des paiements en ligne et des paiements mobiles plus sûrs.

Le système humain de scannage du visage, appelé « Smile and Pay », développé par une filiale d'Alibaba, Ant Financial Services Group, et qui servira pour les paiements en ligne et l'utilisation d'Alipay Wallet, est entré en phase de tests. Mais lors de la cérémonie d'ouverture du salon de l'électronique CeBIT de Hanovre, en Allemagne, le PDG d'Alibaba Jack Ma, a lors de son discours, fait une démonstration de la technologie de paiement facial. Après évoqué les divers problèmes que l'on peut rencontrer lors du paiement en ligne, comme l'oubli du mot de passe, il a utilisé cette technologie de paiement facial devant son auditoire pour acheter un timbre commémoratif du CeBIT de Hanovre.
Selon les données du cabinet de recherche Juniper Research Ltd, en 2019, le volume annuel des paiements en ligne et des paiements mobiles atteindra 4 700 milliards de Dollars US, ce qui fait que les autres entreprises tentent de développer ce service, ainsi d'Apple qui a lancé son service Apple Pay l'année dernière, et Samsung qui a présenté le mois dernier son service Samsung Pay.
Les développeurs de services de paiement mobiles s'efforcent tous de trouver des moyens de payer de façon plus sûre par le biais de technologies d'authentification d'identité. Les iPhone d'Apple utilisent déjà l'identification par empreintes digitales, et le mois dernier, lors du Mobile World Congress, certains fabricants ont présenté une technologie d'identification par scannage oculaire.
De son côté, Alibaba travaille également sur de nouvelles technologies d'identification, ce qui, selon un porte-parole, pourrait peut-être passer par le développement d'une technologie qui permettra aux clients de s'identifier en prononçant une expression particulière, ou même une autre approche appelée « Kung Fu », qui permettra d'identifier un animal domestique en scannant un tatouage.
En outre, le système « Smile to Pay » sera d'abord lancé en Chine, mais, a précisé le porte-parole, la date exacte reste encore incertaine ; il sera ensuite peut-être lancé dans d'autres pays.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://french.peopledaily.com.cn/n/2015/0323/c31357-8867317.html

Paiement par mobiles : Trop peu de sécurité face au piratage

Paiement par mobiles : Trop peu de sécurité face au piratage

Dans ses prédictions de sécurité pour les années à venir, Trend Micro fait un point sur la multiplication des nouveaux moyens de paiement et leur impact potentiel en termes de cybercriminalité.

Le paiement mobile et sans contact
Le lancement d'Apple Pay ou de Google Wallet sont la preuve de l'évolution des usages des consommateurs, désormais prêts à payer directement depuis leur mobile. Cependant, les terminaux mobiles sont toujours peu sécurisés.
Les solutions existantes sont encore trop rarement utilisées par les mobinautes qui n'ont pas pleinement conscience des risques, bien que les cybercriminels ne cessent de perfectionner leurs techniques pour tirer profit de ces nouveaux outils. A titre d'illustration, CurrentC, projet d'un consortium de distributeurs américains pour concurrencer Apple Pay, a récemment été piraté et ce, avant même d'avoir été lancé.

La technologie NFC, largement utilisée dans les solutions de paiement mobile, va ainsi continuer d'être l'objet d'une attention toute particulière des pirates. Les utilisateurs de Google Wallet l'ont déjà appris à leurs dépens lorsqu'une application malveillante, à laquelle des privilèges NFC avaient été accordés, s'est montrée capable de dérober les informations de leur compte utilisateur et leur argent.

« Le NFC s'impose de plus en plus or aujourd'hui, si l'on parle de sécurité, ni les utilisateurs, ni les fabricants d'équipements mobiles ne semblent vraiment prêts », commente Loïc Guézo, de chez Trend Micro. « Les utilisateurs doivent prendre conscience que les attaquants vont se donner les moyens d'intercepter les tags NFC en transit, et se montrer prudents. De leur côté, il est essentiel que les fabricants prennent des mesures et envisagent la sécurité des produits dès leur conception. »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lafibreoptique.com/focus/20112014,cybercriminalite-des-terminaux-mobiles-peu-securises,1920.html