Vtech vend une tablette éducative tout en sachant qu’elle est défectueuse

Vtech vend une tablette éducative tout en sachant qu’elle est défectueuse

Lorsque la fille de 6 ans de Jade a développé son cadeau, le soir du réveillon de Noël, la joie a rapidement cédé la place à la déception.

«Un jouet complètement inutile», «une arnaque». C'est en ces mots que cette mère décrit la tablette Innotab max de Vtech, qui se décrit comme le chef de file mondial en jeux éducatifs électroniques pour enfants.
Le fabricant a confirmé, un peu tard aux yeux de nombreux parents, qu'il s'agissait là d'une conséquence de l'importante cyberattaque dont il a fait l'objet il y a plus d'un mois.

Depuis Noël, la page Facebook de la compagnie a été prise d'assaut par des parents déçus et frustrés de ne pas avoir été mis au courant des problèmes avec la tablette d'apprentissage qu'ils ont payée 120$.
«Quelle déception!», écrit Mélyssa Guay. «Ils auraient dû faire preuve d'honnêteté depuis le début et retirer le produit ou s'assurer que les magasins publient un avertissement», renchérit Samantha Taylor.
«Comme ça coûte cher, c'était le seul cadeau pour ma fille et elle ne peut pas l'utiliser», soupire Jade, avec qui La Presse s'est entretenue. «Il y a des choses pires que ça dans la vie, mais c'est une arnaque de vendre un produit qu'on sait défectueux.»
À mi-novembre, la base de données contenue dans le «Learning Lodge» de VTech, ou «Explor@ Park» en français, a été piratée. Explor@ Park est une plateforme sur laquelle les clients téléchargent les jeux et les vidéos. Ce n'est que deux semaines plus tard, le 30 novembre, que l'entreprise établie à Hong Kong a confirmé le piratage de millions de comptes clients et de profils d'enfants.
Les noms, les dates d'anniversaire des enfants ou les mots de passe et adresses courriel des parents ont été piratés. Mais selon le site Motherboard, du groupe Vice, le pirate a aussi mis la main sur des photos des enfants et des messages. VTech n'a toujours pas confirmé ou démenti cette dernière assertion.

Pas de compte, pas de jeux

La plateforme Explor@ Park a donc depuis été suspendue, ce qui rend impossible l'utilisation de certaines applications pour les tablettes InnoTV, InnoTab MAX, InnoTab. De plus, les nouveaux clients ne peuvent créer de compte. Sans ce compte, le WiFi, les vidéos et les jeux ne sont pas accessibles, ont confirmé des parents à La Presse.
«Je savais qu'il y avait eu une brèche informatique, mais nulle part on ne m'a dit que le produit ne fonctionnerait pas», déplore Jade.
Rachelle Lowry, de Red Deer en Alberta, a acheté une tablette VTech sur le site Amazon le 27 novembre et s'est aperçue il y a deux semaines que rien ne fonctionnait.
«Je leur ai écrit à propos du problème deux semaines avant Noël et je n'ai pas reçu de réponse», a-t-elle expliqué à La Presse. Elle s'est résignée à acheter de nouveaux cadeaux à ses trois enfants pour éviter de les décevoir. «Le service à la clientèle n'a rien fait pour m'aider depuis un mois. Ce n'est qu'à Noël qu'ils ont répondu à mon message Facebook […] C'est très frustrant.»
Le 14 décembre, plus d'un mois après l'attaque informatique, VTech Canada avait écrit sur sa page Facebook un message en anglais pour s'excuser de cet «inconvénient». Le 24 décembre, le fabricant a réitéré ses excuses, ajoutant cette fois une version française.
«Nous nous excusons des inconvénients que cette cyber-attaque et la suspension temporaire à Explor@ Park ont pu vous causer», peut-on lire. Il offre maintenant une solution de rechange, soit le téléchargement d'une mise à jour de programme permettant «de débloquer certaines fonctionnalités encore bloquées sur votre tablette et de bénéficier de 3 JEUX que nous vous offrons pour nous excuser des désagréments rencontrés».
Trop peu trop tard, selon Jade, qui croit qu'un avertissement aurait dû se trouver en magasin. Au commerce Toys'R'Us où elle a acheté le jeu, une préposée lui a affirmé le 26 décembre qu'elle n'était pas au courant du problème. Dans les grandes surfaces où nous nous sommes rendues, la tablette ne se trouvait plus. «Ça s'est beaucoup vendu cette année», a indiqué une vendeuse.

Aucun avertissement

Sur les sites internet de différents détaillants, aucun avertissement n'apparaît. Un message se trouve bien sur le site de VTechkids, mais pas sur la page du produit.
La chaîne Toys'R'Us n'a pas rappelé La Presse hier, pas plus que VTech.
Sur son site internet, le fabricant affirme qu'il espère que certaines des fonctionnalités importantes de la plateforme seront utilisables vers la mi-janvier. Rachelle et Jade attendent toujours que la compagnie leur envoie la carte SD pour effectuer la première mise à jour.
«Mais sur Facebook, j'ai lu que certaines personnes se plaignaient que ça ne fonctionnait pas et je n'ai pas beaucoup d'espoir. Je n'ai plus trop confiance», soupire Jade.

Réagissez à cet article

Source : *Vtech vend une tablette éducative qu'il sait défectueuse | Annabelle Blais | Actualités*

Conférence sur la réponse aux incidents et l'investigation numérique 2016 | CECyF

Conférence sur la réponse aux incidents et l'investigation numérique 2016

Dans le cadre du FIC 2016 – Forum International sur la Cybersécurité, nous vous proposons de nous retrouver le lendemain de cet événement de référence (mercredi 27 janvier 2016), pour la seconde conférence de ce genre en France, dédiée aux techniques de la réponse aux incidents et de l'investigation numérique (retrouver la page de CoRI&IN 2015).

Cette journée, organisée dans les locaux d'Euratechnologies, permettra aux enquêteurs spécialisés, experts judiciaires, chercheurs du monde académique ou industriel, juristes, spécialistes de la réponse aux incidents ou des CERTs de partager et échanger sur les techniques du moment. L'ambition de cette conférence est de rassembler cette communauté encore disparate autour de présentations techniques ou juridiques de qualité, sélectionnées par notre comité de programme.
Si vous souhaitez être tenu informé de l'actualité quant à cette conférence, vous pouvez vous inscrire sur notre liste de diffusion.

Programme prévisionnel

L'accueil sera ouvert le 27 janvier 2015, à partir de 08h30 et la conférence commencera à 9h30, pour se terminer à 16h.
Au 23 décembre 2015, le programme prévisionnel est composé des interventions suivantes:

- Analyse de codes malveillants complexes, Paul Rascagnères et Sébastien Larinier
- La règle du boomerang, Eve Matringe

D'un point de vue juridique, lorsqu'une entreprise ou une institution est victime d'une attaque informatique, quelles sont les marges de manœuvre dont elle dispose pour répliquer? Est-il juridiquement possible de contre-attaquer? Le cas échéant, quels sont les points à envisager?

- De l'hameçonnage ciblé à la compromission totale du domaine, Johanne Ulloa
- Démonstration, état des lieux, limitation du risque et réponse à incident
- Retour d'expérience – gestion de crise SSI en environnement non préparé, Vincent Nguyen
- Surveillance de circonstance, Jean-Baptiste Galet et Alexandre Charlès
- Analyse forensique de dumps de RAM, Pierre Veutin et Nicolas Scherrmann
- Retour d'expérience audit inforensique, Vladimir Kolla

Investigation numérique dans les systèmes industriels : mythe & réalité, David Le Goff

Inscription

Merci de vous inscrire sur la page ci-après (participation aux frais de 10 € et gratuité pour les étudiants – inscription obligatoire):
Les inscriptions sont ouvertes depuis le 07 décembre 2015
https://www.helloasso.com/associations/cecyf/evenements/cori-in

---

Réagissez à cet article

Source : *Conférence sur la réponse aux incidents et l'investigation numérique 2016 | CECyF*

2700 sites Internet suspects passés à la loupe par le ministère de l'Intérieur

2700 sites Internet suspects passés à la loupe par le ministère de l'Intérieur

---

Le ministère de l'Intérieur a présenté au ministère des Technologies de la Communication et de l'Économie Numérique, 2700 requêtes sur des sites et des pages suspectés de prôner le terrorisme, a indiqué ce lundi 28 décembre sur les ondes de Mosaique FM, le ministre des TICS, Noômane Fehri.

Selon le ministre, plusieurs pages sur les réseaux sociaux ont été par ailleurs supprimées sur demandes présentées aux entreprises internationales comme Facebook.
Il a cependant précisé que des sites n'ont pas été supprimés ni masqués afin de pouvoir en extraire des renseignements et de suivre à la trace leurs administrateurs.

Réagissez à cet article

Source : *Cyberterrorisme : 2700 sites suspects ont été passés à la loupe par le ministère de l'Intérieur*

Cyber-attaque contre le ministère des Habous et des affaires islamiques

Cyber-attaque contre le ministère des Habous et des affaires islamiques

Le site du ministère des Habous et des affaires islamiques a été piraté ce Samedi 26 décembre par des hackers se faisant appelé « RxR Hackers. »

Le site du ministère des Habous et des affaires islamiques a été piraté ce Samedi 26 décembre par des hackers se faisant appelé « RxR Hackers. »
Une fois piraté, le site est devenu inaccessible pour les fonctionnaires ainsi que le grand public.
D'après « Le360 », l'attaque est confirmée, et l'ouverture d'une enquête est indispensable pour déterminer les raisons de ce piratage ainsi que l'identité des hackers à l'origine de cet acte qualifié d'irresponsable.

Réagissez à cet article

Source : *Cyber-attaque contre le ministère des Habous et des affaires islamiques – Article 19*

Les données personnelles de 191 millions d’électeurs en accès libre sur la Toile

Les données personnelles de 191 millions d’électeurs en accès libre sur la Toile

---

Un spécialiste en cybersécurité a découvert l’existence d’une base de données contenant les informations personnelles détaillées de 191 millions d’électeurs nord-américains. La fuite serait due à une erreur de configuration de la base de données.

Des données personnelles concernant près de 60% des citoyens des États-Unis se sont retrouvées en libre accès sur la Toile en raison d’un base de données mal configurée. C’est la découverte faite récemment par Chris Vickery, un expert en cybersécurité. La base de données en question n’était apparemment pas sécurisée et serait même toujours active.
Elle contient le nom complet de chaque personne, son sexe, sa date de naissance, son adresse, numéro de téléphone, numéro d’électeur, l’Etat dans lequel elle vote, l’affiliation politique ainsi qu’un historique de ses choix électoraux depuis 2010. Une véritable mine d’or en somme, et Vickery n’a pas indiqué où il avait déniché cette base de données, ni qui en était le créateur.

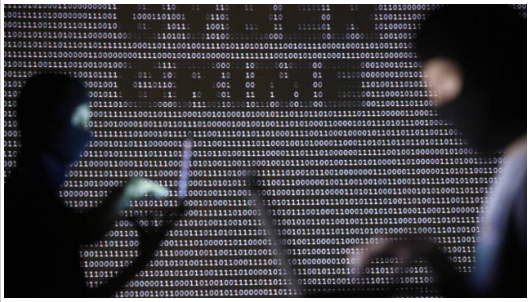
Réagissez à cet article

Source : *États-Unis : les données personnelles de 191 millions d'électeurs en accès libre sur la Toile*

Crainte d'attentats pilotés à partir d'Internet en 2016

Crainte d'attentats pilotés à partir d'Internet en 2016

Les experts en cybercriminalité craignent beaucoup pour l'année à venir. Notamment des attentats déclenchés à distance.



Multiplication des demandes de rançons, perfectionnement des attaques par e-mail, détournement des objets connectés… 2016 ne devrait pas faire chômer les experts de la cybercriminalité, qui craignent de plus en plus un attentat déclenché à distance.

Demandez au bureau du Cercle européen de la sécurité et des systèmes d'information, qui fédère les professionnels du secteur quelle est la plus grande menace planant sur nos têtes, et la réponse sera unanime: « Le #cyber-sabotage, ou #cyber-terrorisme. L'attaque informatique d'un système lourd, qui aura des impacts environnementaux ou humains : polluer l'eau, faire exploser une usine, faire dérailler un train… » Les hackers – États, mafias ou groupes militants – utilisent des méthodes de plus en plus sophistiquées pour « casser » les systèmes informatiques de leurs cibles. À l'exemple de ce haut-fourneau allemand mis hors service il y a un an, on peut tout à fait envisager une cyberattaque contre un équipement vital.

L'éditeur américain Varonis envisage une variante retentissante, une cyberattaque contre la campagne présidentielle américaine. « Elle aura pour conséquence une violation importante des données qui exposera l'identité des donateurs, leurs numéros de carte de crédit et leurs affinités politiques confidentielles », prévoit-il. De quoi provoquer un joyeux désordre.

« Cheval de Troie »

Pour atteindre leurs cibles, les pirates informatiques apprécient particulièrement la technique du « cheval de Troie », qui consiste à faire pénétrer un « malware » (logiciel malveillant) sur les appareils des employés, d'où il pourra progresser vers les unités centrales. Et pour ce faire, une méthode prisée est le « spear phishing », l'envoi de courriels de plus en plus personnalisés, pour amener le destinataire à ouvrir un lien corrompu ou une pièce jointe infectée.

Cette méthode est également utilisée pour faire chanter les gens, chefs d'entreprise ou particuliers, après avoir dérobé et/ou crypter des données – de la comptabilité d'une société aux photos de vacances– qui ne sont rendues et/ou décryptées que contre rançon.

La même méthode peut aussi permettre à une entreprise d'espionner un concurrent. « L'année prochaine, ou dans les deux prochaines années, je pense qu'il va y avoir des vraies affaires qui vont sortir sur le sujet », estime Jérôme Robert, directeur du marketing de la société de conseil française Lexsi.

Smartphones peu protégés

« Il y a beaucoup d'entreprises qui ont déjà utilisé des détectives privés, il n'y a pas de raison qu'elles ne le fassent pas dans le cybermonde », remarque-t-il. Autre préoccupation des spécialistes: le glissement de la vie numérique vers des smartphones qui pèchent parfois par manque de protections.

« Il y a quasiment plus maintenant de smartphones qu'il y a d'ordinateurs, des smartphones qui sont allumés quasiment 24 heures sur 24, qui nous suivent partout », note Thierry Karsenti chez l'éditeur d'antivirus israélien Check Point. « Or, ils ont finalement beaucoup plus de connectivité que les équipements informatiques traditionnels. Ils ont même des oreilles puisqu'il y a un micro, ils ont même une caméra, et ils stockent tout un tas d'informations à la fois professionnelles et personnelles. C'est beaucoup plus embêtant de se faire pirater son smartphone que se faire pirater son ordinateur ! »

« Paradoxalement, si vous regardez la sécurité, vous avez beaucoup plus de sécurité sur un ordinateur », poursuit M. Karsenti. « Alors que les smartphones ou les tablettes n'ont absolument rien en termes de sécurité. » Et le développement des paiements par smartphone devrait allécher les hackers, généralement motivés par l'argent.

Objets connectés détournés

Même préoccupation pour les objets connectés, dont le nombre devrait exploser ces prochaines années. Ceux-ci sont, selon Lam Son Nguyen, expert en sécurité internet chez Intel Security, « souvent conçus sans tenir compte des aspects sécurité ». « Ils vont être susceptibles d'être attaqués par des personnes développant des solutions malveillantes », prévient-il.

Jusqu'à présent, on a surtout vu des hackers s'emparer de données d'utilisateurs stockées sur des serveurs distants des fabricants – dans le « cloud » -, et pas les objets eux-mêmes détournés à distance. « Pour les objets destinés aux consommateurs, il devrait y avoir des attaques qui seront plus des galops d'essai, des jeux, pour se faire plaisir. Je ne vois pas de grosse activité cybercriminelle sur les objets connectés », car il n'y aura sans doute pas d'argent à en tirer dans l'immédiat, juge Jérôme Robert chez Lexsi.

Réagissez à cet article

Source : *Cybercriminalité. Crainte d'attentats déclenchés à distance en 2016*

L’E-réputation, un véritable enjeu pour l’entreprise

	L’E-réputation, un véritable enjeu de pour l’entreprise

En France, 84 % de la population totale ont accès à internet en 2015. Ce chiffre s'élève à 86 % au Canada et à 80 % aux États-Unis. Face à de tels chiffres, force est de constater que les médias traditionnels ne possèdent plus le monopole de l'information de nos jours.

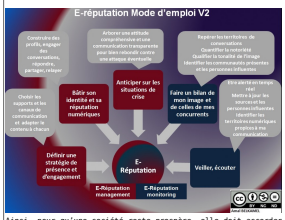
En France, 84 % de la population totale ont accès à internet en 2015. Ce chiffre s'élève à 86 % au Canada et à 80 % aux États-Unis. Face à de tels chiffres, force est de constater que les médias traditionnels ne possèdent plus le monopole de l'information de nos jours.

Ceci entraine de multiples changements pour les sociétés qui souhaitent se forger une image positive ou qui veulent préserver leur statut actuel. L'E-réputation se trouve soudainement au cœur de leurs préoccupations et elle peut leur couter cher si elle est mal entretenue.

Internet, un autre monde

Le temps des médias horizontaux est passé et aujourd'hui, les sociétés doivent combattre sur un nouveau champ de bataille. Ce dernier possède bien entendu des règles totalement différentes. Sur internet par exemple, les clients peuvent désormais se faire entendre par leur semblable. En d'autres termes, ils peuvent détruire une société ou au contraire participer à son essor. Il s'agit d'ailleurs du principal enjeu de l'essor d'internet et de l'e-réputation.

Si une société oublie de prendre soin de son e-réputation, elle risque de vite disparaitre. Attention malgré tout, car même en entreprenant diverses actions sur internet, elles ne seront pas à l'abri d'un « bad buzz ». Pour faire simple, le « bad buzz » correspond à une réponse massivement négative de la part des clients. Dans le meilleur des cas, la société perd quelques parts de marché et dans le pire des cas, elle mettra la clé sous la porte. Comme dit précédemment, les clients peuvent désormais réagir et mener une action en commun afin de mettre à genou une société.



Ainsi, pour qu'une société reste prospère, elle doit accorder une attention particulière à son e-réputation. Pour cela, elle peut commencer par se créer une vitrine sur internet. Elle peut ensuite entreprendre des campagnes marketing ou publicitaire répondant aux codes et aux normes des différentes plateformes sur le web comme les réseaux sociaux. Normes et codes qui, une fois encore, se révèlent différents de ceux des médias traditionnels.

Réagissez à cet article

Source : *E-réputation : un enjeu de taille pour l'entreprise* |

Attention au whaling, ce phishing qui cible les équipes dirigeantes

Attention au whaling, ce phishing qui cible les équipes dirigeantes

---

Selon l'entreprise de sécurité Mimecast, les e-mails conçus pour les attaques de phishing de type whaling, qui ciblent de « gros poissons », sont difficiles à détecter.

Selon l'entreprise de sécurité Mimecast, les e-mails conçus pour les attaques de phishing de type whaling, qui ciblent de « gros poissons », sont difficiles à détecter.
Si vous travaillez dans la finance ou la comptabilité et si vous recevez un email de votre patron vous demandant de transférer des fonds vers un compte externe, mieux vaut réfléchir à deux fois avant d'obtempérer. Selon le cabinet de sécurité Mimecast, ces attaques de phishing très élaborées, dites whaling attacks, qui ciblent des cadres ou des directeurs d'entreprises, mais aussi des personnalités du monde politique ou des personnes célèbres, sont en hausse. Pour camoufler la provenance de e-mails, les pirates utilisent des noms de domaine usurpés ou très proche de domaines familiers du destinataire. Tout est fait pour ce dernier croit que les messages proviennent bien de son directeur financier ou du directeur général.

Le nom de domaine est usurpé dans 70% des attaques

55 % des 442 professionnels IT interrogés par Mimecast ce mois-ci ont déclaré que leur entreprise avait constaté une augmentation du volume de ces « chasses à la baleine » au cours des trois derniers mois, comme l'a déclaré le cabinet de sécurité. Les entreprises visées sont localisées aux États-Unis, au Royaume-Uni, en Afrique du Sud et en Australie. « L'usurpation de nom de domaine est la stratégie la plus courante, puisqu'elle est utilisée dans 70 % des attaques », a précisé le cabinet de sécurité. La majorité des faux messages sont signés du CEO, mais près de 35 % des entreprises ont vu passer des emails signés par le directeur financier. « Les messages conçus pour des attaques de whaling peuvent être plus difficiles à détecter, car ils ne contiennent pas de lien hypertexte ou de pièce jointe malveillante, et comptent uniquement sur l'ingénierie sociale pour tromper leurs cibles », explique Orlando Scott-Cowley, un stratège de la cybersécurité chez Mimecast. « Souvent, des sites comme Facebook, LinkedIn et Twitter fournissent aux attaquants les détails dont ils ont besoin pour préparer ces attaques », a encore déclaré Mimecast.

Informer est la première chose à faire

Alors, que faire ? Mimecast a quelques suggestions. D'abord informer les dirigeants, les équipes de management et de la comptabilité sur ce risque. Ensuite, réaliser des tests sur l'entreprise en montant de fausses attaques de whaling pour évaluer la vulnérabilité des employés. Une autre solution consiste à marquer les emails provenant de l'extérieur du réseau de l'entreprise, ou encore à créer des alertes pour signaler des noms de domaine qui ressemblent étroitement à celui de votre entreprise. « Les barrières pour bloquer l'entrée de ces attaques sont à niveau dangereusement bas », a déclaré Orlando Scott-Cowley. « Étant donné que la pêche est très bonne pour les cybercriminels, il est probable que le volume et la fréquence de ce type d'attaques augmentent », a mis en garde Mimecast.

Réagissez à cet article

Les super cartes bancaires

débarquent

Les super cartes bancaires débarquent

Pour lutter contre la fraude, les banques misent sur la technologie. Demain, on paiera avec une carte à code éphémère ou un smartphone à reconnaissance faciale.

Cette révolution est à portée de main. Dans quelques mois, tout devrait changer… dans votre portefeuille. Votre carte bancaire va s'offrir une deuxième jeunesse. Un relooking qui porte un nom barbare : «cryptogramme dynamique». Ce qui, en français, signifie que les trois petits chiffres, situés au verso de votre carte, changeront au bout de quelques minutes.
Les plus grands fabricants de cartes bancaires au monde, Gemalto et Oberthur, ont lancé ces derniers mois la commercialisation de cette technologie. BNP Paribas, la Banque postale, la Société générale… La quasi-totalité des établissements financiers français sont en train de la tester auprès de leurs clients.

Qui va payer ?
Objectif affiché : mieux lutter contre la fraude à la carte bancaire. Un fléau dont la finance aimerait bien se débarrasser. Pas question de laisser les arnaques et les fraudes nuire à l'engouement des Français pour ce mode de paiement. Imaginez, le 5 décembre dernier, la France a battu un record : 42 millions de transactions par carte bancaire en un week-end. Soit 12 % de plus que lors du premier samedi de décembre 2014 !
Un effet logique du boom du commerce en ligne. Pourtant, les banques se laissent encore quelques mois pour un développement à grande échelle de cette carte bancaire plus sécurisée. Car un petit détail reste encore à trancher. Ce bout de plastique bourré de technologies coûte plus cher à produire que la carte à puce classique. Qui va payer ? La banque, les commerçants ou le client ? Les réponses du milieu bancaire restent floues. Les banques trancheront ces prochains mois. Mais elles n'ont plus vraiment le temps de tergiverser. Des start-up dénommées FinTech (technologie financière) commencent déjà à les bousculer, notamment en utilisant le smartphone pour lancer de nouveaux modes de paiement. Et comme d'autres secteurs l'ont appris à leurs dépens, l'immobilisme face aux nouvelles technologies ne paye pas.
«2016 sera l'année des nouveaux modes de paiements», pronostique donc un cadre de banque. Nombre d'établissements ont, dans les cartons, de nouveaux produits qui n'attendent plus qu'une autorisation de la Cnil (Commission nationale de l'informatique et des libertés) pour passer des simples tests à la commercialisation. C'est le cas des technologies de biométrie utilisant des éléments du corps (empreinte digitale, vocale, etc.). Les bons vieux codes bancaires bientôt périmés ?

Un cryptogramme valable 20 minutes
Même largeur, agilité, finesse, robustesse, touché… A priori, rien ne la distingue de sa prédécesseur. A un détail près : la carte bancaire de nouvelle génération est équipée d'un écran. Tout petit. Pas de quoi regarder un film en haute définition. Non, mais tout de même assez large pour afficher, en noir et blanc, les trois chiffres du fameux cryptogramme visuel. Ce code de sécurité réclamé à chaque achat sur la Toile devient «dynamique». «Cette carte est équipée d'une horloge interne. Le code de sécurité sur l'écran change toutes les vingt minutes», explique Frédérique Richert, marketing manageur chez Gemalto, le leadeur mondial de la carte à puce, qui commercialise depuis quelques semaines cette nouvelle technologie. «Cette carte lutte mieux contre la fraude», ajoute-t-elle.

Réduire le coût des fraudes
A priori, rien ne change pour l'utilisateur. Pour effectuer un achat en ligne, il doit toujours remplir les mêmes formulaires en indiquant son nom, son numéro de carte bancaire, la date de validité et le cryptogramme. La différence, c'est que ces coordonnées ont une durée de vie limitée. Si un pirate informatique les vole, il ne peut alors les utiliser que pendant une vingtaine de minutes. Un laps de temps, a priori, trop court pour multiplier les achats sur le Web ou revendre ces informations à d'autres escrocs.
La plupart des grands réseaux bancaires sont en train de tester auprès de leurs clients cette nouvelle technologie. Ainsi, BPCE a équipé depuis plusieurs semaines un millier de clients. BPCE utilise la technologie d'Oberthur, concurrent de Gemalto. Avec un avantage, celui de réduire le coût des fraudes. Car les banques assument une partie du coût de l'arnaque : indemnisation du client pour les achats réalisés frauduleusement, coût du changement du support, etc. «Nous regardons à la fois l'effet de cette nouvelle technologie sur le coût lié à la fraude mais aussi sur la confiance des utilisateurs dans le paiement en ligne, dans l'usage des cartes bancaires», explique Nicolas Chatillon, directeur du développement fonctions transverses du groupe BPCE. Un point stratégique. Car un possesseur de carte bancaire en confiance, c'est un consommateur qui dépense !

Réagissez à cet article

Source : *Les super cartes bancaires débarquent*

Paralyser une voiture pour 90 euros | Data Security Breach

Paralyser une voiture pour 90 euros | Data Security Breach

---

la prise USB d'une Toyota Corolla, un chercheur en informatique, bloque la voiture à coup de DDoS.

Le monde du « sans connexion » envahi nos vies. La marche de l'IoT est lancée et rien ne l'arrêtera vue les enjeux économiques. L'important, que le client achète, on verra ensuite pour sa sécurité. **Du moins si le client est encore vivant.**

Inoue Hiroyuki, professeur en informatique à la Graduate School of Information Sciences de l'université d'Hiroshima a expliqué comment il avait « planté » une Toyota Corolla avec 90€.
Une clé USB trafiquée et un DDoS via le port USB de la voiture « Le pilote était incapable de bouger la voiture en appuyant sur l'accélérateur » explique-t-il dans le Japan Times. L'agrégé en informatique a indiqué avoir aussi été capable d'ouvrir et fermer les fenêtres de la voiture, afficher une lecture de compteur de vitesse incorrecte et geler l'accélérateur. Toyota a annonçait qu'il allait continuer « à faire des efforts » pour améliorer la sécurité de ses véhicules.

Il serait peut-être temps d'arrêter de nous prendre pour des idiots ?
En juillet 2015, une Jeep Cherokee, et un mois plus tard, une Corvette étaient elles aussi malmenées. Le piratage des voitures ne fait que débuter ! Pour le moment, il ne se déroule officiellement que dans des laboratoires.

Réagissez à cet article

Source : *Paralyser une voiture pour 90 euros | Data Security Breach*