52 % des DSI Français acceptent moins de sécurité pour plus de mobilité

C’est une nouvelle à la fois peu surprenante et inquiétante : plus de la moitié des responsables informatiques en France cèdent du terrain sur le plan sécuritaire pour avantager la mobilité et le Bring Your Own Device.

« **Rendre les salariés et les opérations plus agiles** »
On ne cesse de le répéter depuis des années : le BYOD est loin d’être toujours un choix, il n’est pas rare qu’il s’impose de lui-même. Rejeter cette situation, c’est risquer une utilisation sous-marine, multipliant ainsi les risques. L’accepter, c’est limiter les risques en question en encadrant le BYOD.
Dans une étude menée par le cabinet Vanson Bourne pour le compte de VMware (plus de détails en fin d’article), nous apprenons que 52 % des responsables informatiques français font face à une telle pression vis-à-vis de la mobilité d’entreprise « qu’ils sont prêts à prendre des risques inconsidérés vis-à-vis de la sécurité des données de leur organisation ».
Ces risques sont en grande partie pris pour contenter les cadres dirigeants qui souhaitent absolument accéder aux données pro via leurs propres terminaux, « même si cela va à l’encontre des stratégies de leur entreprise » et que cela multiplie les risques de cyberattaques.
Mais les gains en valent la chandelle puisque les DSI cèdent. 51 % d’entre eux estiment ainsi que les bénéfices sont supérieurs aux risques. « Transformation numérique et mobilité sont indissociables. Les organisations doivent sans cesse chercher à développer leurs activités et à innover. Elles prennent donc des risques à court terme sur le plan de la sécurité afin de rendre les salariés et les opérations plus agiles » explique notamment Sylvain Cazard, directeur général de VMware France.
Pour s’adapter au marché et aux désirs de certains salariés, les DSI n’hésitent donc pas à prendre plus de risques. Il faut dire que près d’un quart des responsables informatiques estiment que le manque de mobilité des salariés réduit leur productivité. Un argument qui fait mouche et pousse logiquement les DSI à lâcher du lest côté sécurité.

Des salariés mal formés, des patrons sous-informés
Bien évidemment, les responsables n’ont pas à laisser la porte ouverte au premier pirate informatique venu. Une plus forte pédagogie auprès des salariés devient ainsi indispensable si l’entreprise ne souhaite pas voir toutes ses données partir dans la nature. Ce point est d’autant plus majeur sachant que l’étude indique que 60% des salariés mobiles précisent ne pas connaître la politique de sécurité de leur entreprise… Une statistique douloureuse et effrayante qu’il convient de ne pas minimiser.
Plus grave encore pour les dirigeants d’entreprises, une ancienne enquête de Vanson Bourne montrait que 25 % des DSI français ont confié ne pas informer leur patron en cas de cyberattaque. Ceci alors même que 29 % des DSI et 21 % des employés estiment que leurs patrons sont responsables en cas de fuite de données. Une incohérence qui en dit long sur la complexité de la problématique…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l’étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d’un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : BYOD : 52 % des DSI

Français acceptent moins de sécurité pour plus de mobilité

Pourquoi les vols de données sont en forte hausse ?

	Pourquoi les vols de données sont en forte hausse ?

Une étude du Ponemon Institute pour Varonis révèle que la plupart des collaborateurs disposent d'accès trop importants, ce qui multiplie les dommages lorsque leurs comptes sont compromis

Trois entreprises sur quatre ont été victimes de la perte ou du vol de données importantes au cours des deux dernières années. Selon une nouvelle enquête menée auprès de plus de 3 000 collaborateurs et informaticiens aux États-Unis et en Europe, cela représente une très forte augmentation depuis 2014. Le rapport publié aujourd'hui a été rédigé par le Ponemon Institute et sponsorisé par Varonis Systems, Inc., principal fournisseur de solutions logicielles permettant de protéger les données contre les menaces internes et les cyberattaques.
Selon l'enquête, l'augmentation de la perte et du vol des données est en grande partie due aux compromissions de comptes internes. Celles-ci sont aggravées par des accès aux informations critiques bien plus permissifs que nécessaire par les collaborateurs et les tiers. Sans oublier le constant défaut de supervision des accès et de l'activité dans les systèmes de messagerie et les systèmes de fichiers, là où se trouvent les données les plus sensibles et les plus confidentielles.
Parmi les principales conclusions :
• 76 % des informaticiens indiquent que leur entreprise a fait l'expérience de la perte ou du vol de ses données au cours des deux dernières années. Ce chiffre représente une augmentation importante par rapport aux 67 % d'informaticiens interrogés ayant donné la même réponse lors de l'étude de 2014 réalisée par Ponemon pour le compte de Varonis.
• Les informaticiens indiquent que la négligence des collaborateurs a deux fois plus de chances d'entraîner la compromission des comptes internes que tout autre facteur, y compris les attaquants externes ainsi que les collaborateurs ou les prestataires malveillants.
• 78 % des informaticiens déclarent être très préoccupés par les ransomware, un type de logiciels malveillants qui bloque l'accès aux fichiers jusqu'au paiement d'une somme d'argent. 15 % des entreprises ont déjà fait l'expérience des ransomware et seule une petite moitié d'entre elles a détecté l'attaque au cours des 24 premières heures.
• 88 % des utilisateurs finaux indiquent que leur travail exige l'accès et l'emploi d'informations propriétaires telles que des données relatives aux clients, des listes de contacts, des renseignements sur les collaborateurs, des rapports financiers, des documents commerciaux confidentiels ou d'autres actifs informationnels critiques. C'est nettement plus que les 76 % enregistrés dans l'étude de 2014.
• **62 % des utilisateurs finaux indiquent avoir accès à des données de l'entreprise qu'ils ne devraient probablement pas pouvoir consulter**.
• Seuls 29 % des informaticiens interrogés indiquent que leur entreprise applique un modèle strict de moindre privilège pour s'assurer que les collaborateurs ont accès aux données de l'entreprise en fonction de leur besoin de les connaître.
• Seulement 25 % des entreprises supervisent toute l'activité relative à la messagerie et aux fichiers, alors que 38 % ne supervisent aucune activité.
• 35 % des entreprises ne disposent d'aucun enregistrement interrogeable de l'activité du système de fichiers, ce qui les rend incapables de déterminer les fichiers chiffrés par ransomware (entre autres choses).
Le rapport d'étude intitulé *« Closing Security Gaps to Protect Corporate Data: A Study of U.S. and European Organizations »* se fonde sur des entretiens menés en avril et mai 2016 auprès de 3 027 employés aux États-Unis, au Royaume-Uni, en France et en Allemagne. L'ensemble des personnes interrogées comprend 1 371 utilisateurs finaux ainsi que 1 656 informaticiens et professionnels de la sécurité informatique issus d'entreprises de tailles variant de quelques douzaines à plusieurs dizaines de milliers d'employés. Ils proviennent de divers secteurs, dont les services financiers, le secteur public, le secteur des soins de santé et des sciences de la vie, la vente au détail, le secteur industriel, le secteur technologique et l'industrie du logiciel…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Vols de données en forte hausse, cause principale: les menaces internes | Docaufutur

---

Enfin un outil pour savoir si votre webcam n’est pas piratée

Enfin un outil pour savoir si votre webcam n’est pas piratée

L'outil, Oversight, alerte les utilisateurs d'un Mac d'une tentative de contrôle à distance de leur webcam, lors d'une session vidéo légitime.

Masquer la webcam de son ordinateur est une méthode low-tech contre les techniques d'espionnage consistant à activer à distance la caméra d'un ordinateur. Une méthode très utilisée, le directeur du FBI et le président de Facebook peuvent en témoigner… Dévoilé cette semaine, lors de la conférence Virus Bulletin de Denver, l'outil Oversight, conçu par Patrick Wardle, directeur de recherche de Synack et ancien employé de la NASA et de la NSA américaine, vise à déjouer le piratage potentiel des webcams sous OS X par un malware.

Oversight plus fort que le LED ?

Ce type de programme malveillant peut surveiller discrètement le système et repérer les sessions vidéo initiées par l'utilisateur du Mac, selon Wardle. Par exemple, lors d'une communication utilisant FaceTime ou Skype. Le malware peut alors enregistrer les sessions vidéo et audio, sans être repéré. Car l'indicateur LED de l'appareil est déjà allumé pour signaler que la webcam est active…

Oversight notifie l'utilisateur lorsqu'une application tente d'accéder à la webcam et au microphone intégré. C'est à l'utilisateur de décider de maintenir le flux vidéo, ou de le bloquer. Si un malware présent dans le système est conçu pour agir lorsque la webcam et le micro sont activés par l'utilisateur, Oversight est censé lancer deux notifications : l'une lorsque des applications légitimes de communication se lancent, l'autre lorsque le logiciel malveillant est activé…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Un outil pour vérifier que votre webcam n'est pas détournée

Arte utilise l'Intelligence Artificielle pour répondre aux téléspectateurs

Arte utilise l'Intelligence Artificielle pour répondre aux téléspectateurs

La chaîne de télévision franco-allemande ARTE souhaite déployer un « Bot apprenant » pour répondre aux questions courantes de ses téléspectateurs.

Bot – Dans le prolongement du hackathon en ligne, proposé en juin dernier et conjointement avec Microsoft, ARTE a lancé, avec l'équipe gagnante, le développement d'un « Bot apprenant » capable de répondre rapidement et avec pertinence aux questions les plus courantes de ses téléspectateurs. Ce nouvel outil conversationnel devra permettre à ARTE d'instaurer un nouveau type de relation avec son public, fondé sur la permanence et l'ubiquité de ses services. Porté par les solutions d'Intelligence Artificielle de Microsoft, ce nouveau Bot va, à termes, simplifier l'accès aux programmes de la chaîne, enrichir l'expérience des téléspectateurs et favoriser les échanges…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Bot : L'Intelligence Artificielle au service de la relation avec les téléspectateurs d'Arte – Data Security BreachData Security Breach

Quelles failles pour les voitures connectées ?

	Quelles failles pour les voitures connectées

L'édition du salon de l'auto interpelle le grand public sur les nouveaux pirates de la route. Voitures connectées : les cybercriminels dans l'angle mort ?

Nul doute, la voiture connectée est encore l'une des stars du salon de l'auto cette année. Comme tout ce qui attrait à internet et aux objets connectés, il est légitime de se poser quelques questions notamment sur la sécurité liée au partage des données ainsi qu'à cette forme de déplacement autonome. Un véhicule connecté est en effet doté d'un accès à Internet ainsi que, plus généralement, d'un réseau local sans fil. L'accès Web offre divers services supplémentaires tels que la notification automatique des embouteillages, la réservation de parking, la surveillance du style de conduite (pouvant par ailleurs avoir une incidence sur le montant des primes d'assurance automobiles) etc.
De multiples raisons peuvent motiver les cybercriminels à tenter de pirater des voitures connectées :
L'appât du gain : ll s'agit de bloquer l'accès au véhicule jusqu'à ce la victime paie une rançon.
L'espionnage : l'activation du micro ou de la caméra équipant le véhicule peut donner accès à des informations exclusives et des données sensibles.
La violence physique : les attaques peuvent avoir pour but de blesser le conducteur, ses passagers, ou encore d'endommager d'autres véhicules sur la route.
C'est en analysant ses raisons que la société russe développe une approche de la sécurité interne des véhicules connectés. Elle reposent sur deux principes : D'abord l'isolement veille à ce que deux entités indépendantes (applications, pilotes, machines virtuelles) ne puissent interférer l'une avec l'autre en aucune façon. Ensuite, le contrôle des communications signifie que deux entités indépendantes ayant à communiquer dans le système doivent le faire conformément à des règles de sécurité. L'utilisation de techniques de cryptographie et d'authentification pour l'envoi et la réception des données fait également partie intégrante de la protection du système.
Pour respecter notre travail, merci de ne reprendre que l'intro. Pour lire la suite de cet article original direction -> http://www.datasecuritybreach.fr/voitures-connectees-cybercriminels-langle-mort/#ixzz4MV1xJas6

Follow us: @datasecub on Twitter
…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Voitures connectées : les cybercriminels dans l'angle mort ? – Data Security Breach

FakeAlert : Découverte d'une infection qui touche la France

FakeAlert : Découverte d'une infection qui touche la France

Détection d'une très forte augmentation du nombre d'échantillons du malware HTML / FakeAlert, à destination de la France.

HTML / FakeAlert est le nom générique donné par l'éditeur de solution de sécurité informatique ESET. Un terme qui nomme les fausses pages web hébergeant des messages d'alertes. Ces derniers indiquent à l'utilisateur qu'il est infecté par un virus ou qu'il a un autre problème susceptible de compromettre son ordinateur ou ses données. Pour stopper la soi-disant menace, l'utilisateur est invité à contacter par téléphone le faux support technique ou à télécharger une fausse solution de sécurité.
Le malware HTML / FakeAlert est généralement utilisé comme point de départ pour ce que l'on appelle les escroqueries de faux support. En conséquence, les victimes perdent de l'argent (en appelant des numéros surtaxés ou internationaux) ou sont infectés par un vrai malware installé sur leur ordinateur via les programmes « recommandés » figurant sur la page des fausses alertes…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : FakeAlert : Découverte d'une infection qui touche la France – ZATAZ

Gestion des mots de passe : Où en sont nos comportements ?

	Gestion des mots de passe : Où en sont nos comportements ?

Les internautes ont conscience du risque. Malgré tout, 61 % réutilisent les mêmes mots de passe sur différents comptes, selon une enquête internationale de Lab42 pour LastPass.

Malgré les recommandations en faveur de l'utilisation de mots de passe robustes, malgré la médiatisation de violations de données à grande échelle (Yahoo, LinkedIn…), la réutilisation de mots de passe aisément mémorisables est une pratique courante. C'est le principal enseignement d'un sondage réalisé par la société d'études Lab42 pour le gestionnaire de mots de passe LastPass.
L'enquête a été menée en mai dernier auprès d'un échantillon de 2000 internautes majeurs dans 6 pays : France, Allemagne, Royaume-Uni, États-Unis, Nouvelle Zélande et Australie.

Déni et prise de risque

Malgré la compréhension du risque (pour 91 % du panel), 61 % des internautes interrogés réutilisent les mêmes mots de passe sur différents comptes, sites et services en ligne. Autre enseignement du sondage : l'oubli d'un mot de passe est la principale raison à l'origine d'un changement. Seulement 29 % des personnes interrogées changent de mot de passe pour des raisons de sécurité.
La majorité rationalise le fait d'utiliser des mots de passe *« faibles »*. Près de la moitié des répondants (identifiés comme des personnalités de Type A par le Lab42) veulent garder le contrôle et mémoriser les mots de passe utilisés. Ils pensent ainsi ne pas être directement menacés.
En revanche, plus de 50 % des répondants (identifiés comme des personnalités de type B) disent limiter leur activité en ligne par crainte d'une violation de mots de passe. Ils parviennent à se convaincre que leurs données n'ont pas de valeur pour les hackers. Et maintiennent ainsi une approche distante, voire négligente en ce qui concerne la sécurité des mots de passe…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Mots de passe : le déni et la prise de risque exposés

Yahoo espionne tous vos e-mails pour le compte de la NSA ou du FBI

Yahoo espionne tous vos e-mails pour le compte de la NSA ou du FBI

Yahoo a accepté sans combattre d'installer un logiciel sur ses serveurs, qui regarde le contenu des e-mails qui arrivent et transmet aux services de renseignement américains ceux qui peuvent les intéresser. Il est plus que temps de fermer son compte Yahoo.

L'agence Reuters a révélé mardi que les ingénieurs en charge du service des e-mails de Yahoo ont développé et mis en place en 2015 un logiciel qui scanne le contenu de tous les messages envoyés vers les centaines de millions de comptes Yahoo, pour copier et mettre à la disposition des autorités américaines ceux qui contiennent certaines chaînes de caractères intéressant les services de renseignement. L'ordre confidentiel, qui émanerait de la NSA ou du FBI et a été confirmé par quatre sources dont trois anciens employés de Yahoo, a été suivi sans que la direction de Yahoo le conteste.
C'est la découverte du bout de code qui aurait conduit le chef de la sécurité de Yahoo, Alex Stamos, à démissionner et partir chez Facebook en juin 2015. Ses équipes n'avaient pas été informées et il jugeait que le code mettait en danger la sécurité des utilisateurs…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Yahoo espionne tous vos e-mails pour le compte de la NSA ou du FBI — Tech — Numerama

Un sous-traitant de la NSA accusé de vol de données secrètes

	Un sous-traitant de la NSA accusé de vol de données secrètes

’affaire est embarrassante pour la National Security Agency (NSA). Le ministère américain de la justice a annoncé, mercredi 5 octobre, l’arrestation d’un homme soupçonné d’avoir volé des données classées « top secret » alors qu’il travaillait pour une agence fédérale, identifiée comme la NSA par le New York Times.

L’homme arrêté, Harold Thomas Martin III, travaillait comme sous-traitant à l’agence de renseignement américaine, spécialisée dans l’espionnage des communications mondiales. Il était employé par Booz Allen Hamilton, un grand groupe privé américain qui fournit de nombreux sous-traitants aux agences du renseignement des Etats-Unis.
« Lorsque nous avons appris l’arrestation de notre employé, nous avons immédiatement joint les autorités fédérales pour proposer notre totale coopération, et nous avons licencié » le sous-traitant, a confirmé, mercredi, dans un communiqué Craig Veith, le vice-président de Booz Allen Hamilton.

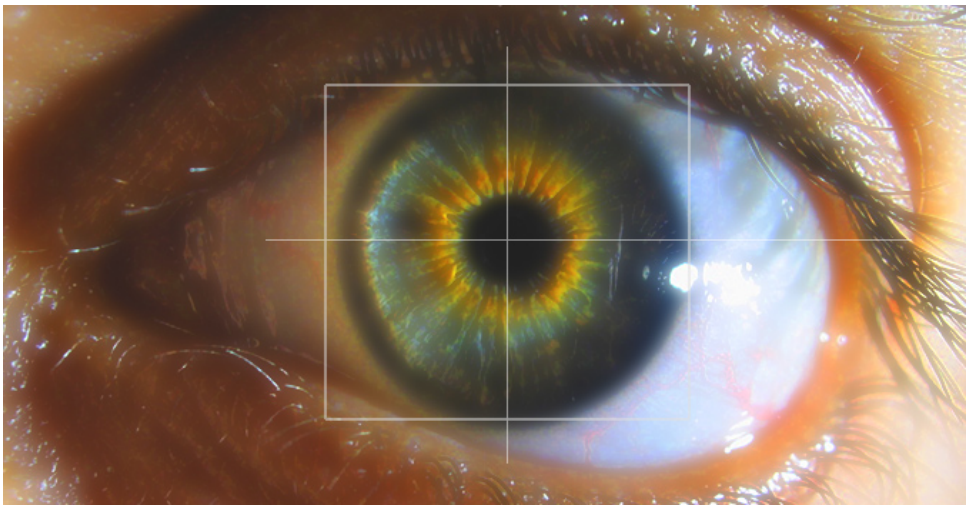
Embarrassant pour la NSA

Pour la deuxième fois en trois ans, la NSA voit l’un de ses sous-traitants dérober des informations ultrasecrètes. Edward Snowden, qui a révélé au grand public l’ampleur des programmes de surveillance de la NSA, était également un sous-traitant de Booz Allen Hamilton. La NSA n’a pas répondu aux sollicitations de l’Agence France-Presse.
Selon le *New York Times*, M. Martin est *« soupçonné d’avoir pris les codes source très secrets développés par la NSA pour s’introduire dans les systèmes informatiques d’adversaires comme la Russie, la Chine, l’Iran et la Corée du Nord »*.
L’acte d’accusation se borne à mentionner que M. Martin a emporté chez lui du matériel informatique et des documents confidentiels qui n’auraient jamais dû sortir du bureau où il travaillait. Il encourt respectivement un an et dix ans de prison pour ces faits, selon la même source.
[Source : Le Monde]

Réagissez à cet article

Original de l’article mis en page : Etats-Unis : un sous-traitant de la NSA accusé de vol de données secrètes

MasterCard déploie le paiement par selfie



MasterCard déploie le paiement par selfie

Après une phase de test dans quelques pays, le paiement par selfie imaginé par MasterCard se déploie en Europe.

C'est une procédure que vous connaissez forcément si vous avez déjà eu l'occasion d'effectuer un achat en ligne. Au moment du paiement, la boutique vous demande de renseigner les informations de votre carte bancaire (son numéro, sa date d'expiration et son cryptogramme visuel).
Une fois ces informations envoyées, votre banque est censée vous envoyer un SMS de confirmation contenant un code qu'il faut inscrire sur le site du marchand afin de valider définitivement la transaction. Cette mesure est nécessaire en cas de vol de la carte, afin de neutraliser toute tentative d'utilisation frauduleuse.
Avec l'envoi d'un code par texto (ou par mail), le client limite déjà beaucoup le risque de se faire avoir. Mais la méthode ne contre pas 100 % des menaces. Des fraudeurs très motivés et compétents peuvent modifier le numéro de téléphone censé recevoir le code ou accéder à la boîte mail pour y recevoir le courrier de validation. C'est en ayant ces problématiques en tête que MasterCard tente une autre approche, avec l'utilisation du selfie.

Évidemment, des interrogations apparaissent : que se passe-t-il si on utilise une photo de moi ? MasterCard dit avoir trouvé une parade en demandant à l'usager, pendant le selfie, de cligner des yeux. Et si une vidéo de moi est utilisée alors ? La parade pourrait être plus difficile à trouver, mais encore faut-il que le fraudeur puisse obtenir une vidéo de la victime, de face, en train de cligner des yeux. Or, elle n'existe peut-être pas.
Et quid des données biométriques qui sont par nature hautement sensibles ? MasterCard assure au Figaro qu'aucune information de cette nature n'est récupérée par le groupe sous sa forme originale. Manifestement, l'image est convertie en une sorte de signature numérique, qui est ensuite transmise à l'entreprise sans que celle-ci ne soit en mesure de faire le chemin inverse pour reconstituer le visage…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Le paiement par selfie de MasterCard se déploie en Europe – Tech – Numerama