

Les 15 mesures clés de la loi Numérique



Les 15
mesures
clés de
la loi
Numérique

Vous n'avez guère suivi les débats autour du projet de loi Numérique, qui vient tout juste d'être définitivement adopté par le Parlement ? Voici un panorama de quinze mesures emblématiques. Élan en faveur de l'Open Data...[Lire la suite]

Denis JACOPINI anime des **conférences**, des **formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en **protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

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]

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 la 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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

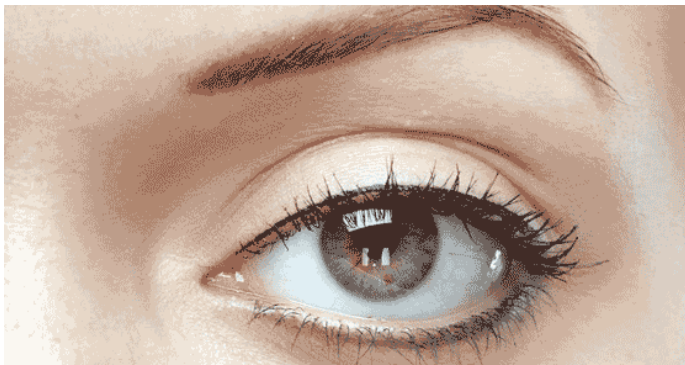


[Contactez-nous](#)

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 la 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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



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 attire 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 : il 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 repose 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>

Under Creative Commons License: Attribution Non-Commercial No Derivatives

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 la 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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



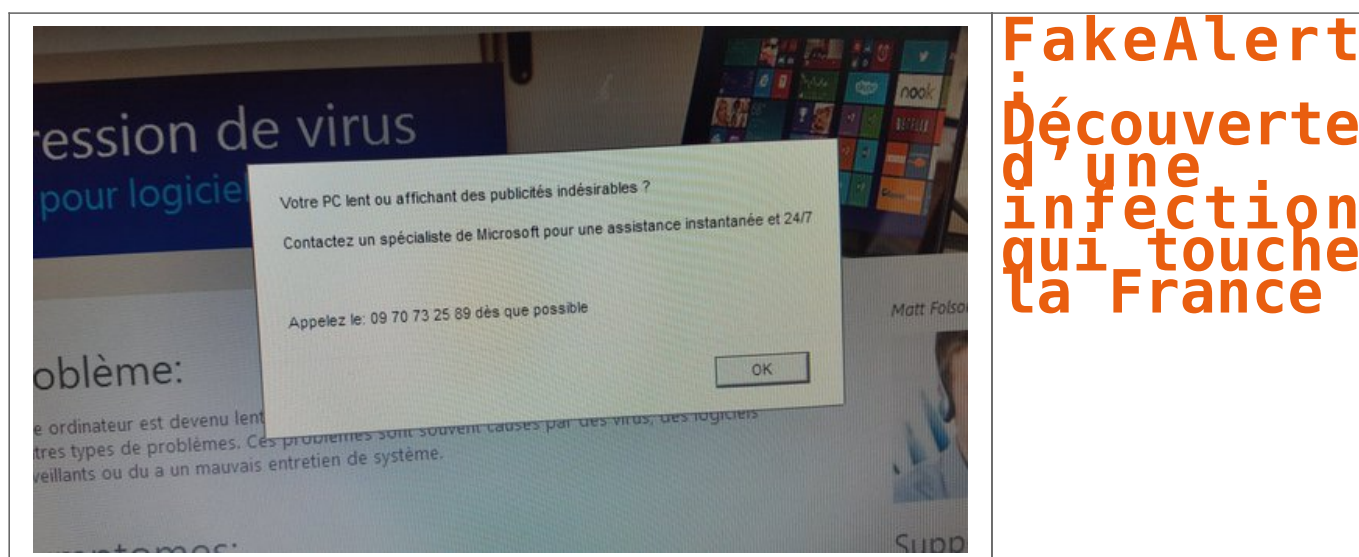
[Contactez-nous](#)



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



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 la 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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

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

Alerte : le gestionnaire de mots de passe SplashID piraté



Alerte : le
gestionnaire
de mots de
passe
SplashID
piraté

Le gestionnaire de mots de passe SplashID a été victime d'un piratage. Une base de données complète lui appartenant est en vente sur le Dark Web.

SplashID victime d'un piratage d'envergure

Alors qu'en début d'année, c'est le gestionnaire de mots de passe de Trend Micro qui avait vu son image écorner après la découverte de nombreuses failles dans ce logiciel, voilà qu'un concurrent vient de connaître pareille mésaventure.

Eh oui, au cours des derniers jours semble-t-il, SplashID a été victime d'un très vaste piratage qui a permis à des hackers, probablement en exploitant des failles décelées au niveau du coffre-fort numérique, de dérober la base de données complète du gestionnaire de mots de passe.

C'est d'ailleurs celle-ci qui a été retrouvée sur le Dark Web au prix de 8,5 bitcoins soit un peu plus de 4600€.

Un gestionnaire de mots de passe en ligne qui montre ses limites

Si les services comme SplashID peuvent sembler très pratiques puisqu'il est possible de s'y connecter très simplement depuis n'importe quel terminal, fixe ou mobile, ils présentent toutefois d'importants risques sur le plan sécuritaire.

Eh oui, parce que ce type de services est en ligne, il est potentiellement exposé à de nombreuses menaces alors qu'un service hors-ligne est par essence plus sécurisé.

Reste que dans l'affaire SplashID, l'inquiétude des internautes est grande puisque la société qui gère le service ne s'est pour l'instant pas exprimée à propos du piratage dont elle a été victime. Or, les rumeurs laissent entendre que les cybercriminels détiendraient encore un accès dérobé au serveur à ce jour !...[lien vers l'article informanews]

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 la 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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Mise à disposition de l'outil de déchiffrement contre le ransomware Polyglot



Les victimes du ransomware Polyglot, aussi connu sous le nom MarsJoke, peuvent maintenant récupérer leurs fichiers grâce à l'outil de déchiffrement développé par Kaspersky Lab.

Comment fonctionne Polyglot ? Il se propage via des emails de spam qui contiennent une pièce jointe malicieuse cachée dans une archive RAR. Durant le processus de chiffrement, il ne change pas le nom des fichiers infectés mais en bloque l'accès. Une fois le processus de chiffrement terminé, le wallpaper de bureau de la victime est remplacé par la demande de rançon. Les fraudeurs demandent que l'argent leur soit remis en bitcoins et si le paiement n'est pas fait dans les temps, le Trojan se détruit en laissant tous les fichiers chiffrés.

Lien avec CTB-Locker ?

Le fonctionnement et le design de ce nouveau ransomware sont proches de ceux de CTB-Locker, un autre ransomware découvert en 2014 qui compte de nombreuses victimes à travers le monde. Mais après analyse, les experts de Kaspersky Lab n'ont trouvé aucune similarité dans le code. En revanche, contrairement à CTB-Locker, le générateur de clés de chiffrement utilisé par Polyglot est faible. Les créateurs de Polyglot semblaient penser qu'en imitant CTB-Locker, ils pourraient piéger les utilisateurs en leur faisant croire qu'ils étaient victimes d'un grave malware, ne leur laissant d'autre option que de payer...[Téléchargez l'outil]

Article de Data Security Breach

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 la 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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Outil de déchiffrement contre le ransomware Polyglot – Data Security Breach
Data Security Breach

L'accord Privacy Shield entre en vigueur

	L'accord Privacy Shield entre en vigueur
---	---

[par le Général d'armée (2S) Marc Watin-Augouard, Fondateur du FIC et Directeur du CRE0GN]

Il y a quelques semaines, le Privacy Shield vient d'être adopté en remplacement du Safe Harbor. Cet accord, relatif à la protection des données à caractère personnel des Européens, est un progrès, même s'il suscite des réserves de la part du G29. Sa révision en 2017 sera l'occasion de faire un premier bilan.

Les principes du Safe Harbor ont été établis pour protéger les données à caractère personnel, conformément aux dispositions de l'ancienne directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, encore en vigueur jusqu'au 25 mai 2018. Celle-ci impose un niveau élevé de protection des droits et libertés des personnes, équivalent dans tous les États membres, en particulier pour permettre la libre circulation de leurs données à l'intérieur de l'Espace économique européen (EEE). Elle interdit le transfert de données à caractère personnel vers un pays tiers, lorsque celui-ci n'offre pas un « niveau de protection adéquat ».

La décision d'adéquation du 26 juillet 2000 de la Commission 2000 relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » reconnaissait que les transferts entre l'Union et les États-Unis répondaient aux conditions. La décision ne visait pas le secteur financier ou bancaire concerné par l'accord SWIFT[1]. Elle ne s'appliquait pas non plus lorsque sont établies des règles internes de transfert de données (Binding Corporate Rules ou BCR) validées par les 28 régulateurs nationaux (à vrai dire un seul en vertu du principe de reconnaissance mutuelle), des « clauses contractuelles types » élaborées par la Commission européenne, ou lorsque le transfert répond aux conditions définies par l'article 69 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[2].

La décision de la Commission a été annulée par l'arrêt CJUE C-360/14 Maximilian Schrems/ Data Protection Commissioner du 6 octobre 2015. L'arrêt concernait plus de 4000 entreprises américaines implantées en Europe directement affectées par ses conséquences. Tout en étant salué par les défenseurs des droits de l'internaute, il inquiétait les milieux économiques, notamment les PME. Celles-ci ne disposent pas, en effet, de services juridiques suffisamment étoffés pour établir des clauses contractuelles type, des règles internes d'entreprises, ou d'obtenir des autorisations de la CNIL (art.69 de la loi du 6 janvier 1978) prévoyant le transfert de données hors du Safe Harbor.

Le 26 octobre, la commissaire européenne à la Justice, Vera Jourová, annonce un « Safe Harbor II », preuve que l'urgence est prise en compte. La Commission, sommée de présenter un nouvel accord avant le 31 janvier 2016, accélère les négociations (déjà engagées auparavant) en vue d'aboutir à un texte pouvant être jugé satisfaisant, notamment par le G29. Elle présente ainsi, le 29 février 2016, son projet de « décision sur le caractère adéquat du niveau de protection », ainsi que les textes (Privacy Shield Principles) qui composeront le « bouclier de protection des données UE-États-Unis ».

Les grandes lignes du Privacy Shield peuvent être ainsi résumées :

1/ Les entreprises seront soumises à des obligations assorties de mécanismes de surveillance permettant de les sanctionner ou de les exclure. Les nouvelles règles comprennent également des conditions plus strictes pour les transferts à d'autres partenaires par les entreprises adhérant au dispositif.

2/ L'accès par les autorités américaines sera étroitement encadré et transparent: le gouvernement américain, par la voix du directeur du renseignement national, a donné par écrit des garanties à l'UE. Tout accès des pouvoirs publics aux données à des fins de sécurité nationale sera subordonné à des limitations, des conditions et des mécanismes de supervision bien définis, qui empêcheront un accès généralisé aux données personnelles. Un mécanisme de médiation, indépendant des services de sécurité nationale, sera mis en place.

3/ La protection des citoyens de l'UE sera mieux assurée par un mécanisme de règlement extrajudiciaire des litiges, accessible sans frais. Les entreprises visées devront apporter une réponse aux plaintes dans les 45 jours. Les citoyens de l'UE pourront également s'adresser à leur autorité nationale chargée de la protection des données, qui collaborera avec la Federal Trade Commission (Commission fédérale du commerce), un mécanisme d'arbitrage étant disponible, en dernier ressort, pour trouver une solution.

4/ Un examen annuel conjoint sera opéré par la Commission européenne et le ministère américain du commerce, associant des experts travaillant au sein des autorités américaines et européennes de protection des données. La Commission organisera une rencontre annuelle avec des ONG et des parties prenantes dans le domaine du respect de la vie privée, pour débattre de l'évolution plus générale de la législation américaine sur la vie privée et de ses répercussions pour les citoyens européens. Elle adressera un rapport annuel public au Parlement européen et au Conseil.

Après la promulgation par Barack Obama, le 24 février, de la loi sur le recours juridictionnel (Judicial Redress Act[3]), la Commission ouvre la procédure de signature de l'accord-cadre. Le dispositif doit être adopté par le Collège des commissaires européens, après consultation d'un comité composé de représentants des États membres et après avis des autorités européennes chargées de la protection des données (G29). Entre-temps, les États-Unis doivent mettre en place le nouveau cadre et les mécanismes de contrôle et de médiation. Le 13 Avril 2016, le G29 a fait savoir, par la voix de sa présidente Isabelle Falque-Pierrotin, que le texte constitue une avancée encore perfectible.

La décision sur la conclusion de l'accord est adoptée par le Conseil, le 12 juillet 2016, après approbation du Parlement européen. Elle entrera en vigueur dès sa notification aux États membres. Le 25 juillet 2016, le G29 se réunit et maintient sa position. Parmi les points suscitant les critiques, l'absence de garanties sur l'abandon de la surveillance massive des données des Européens par les services américains, les doutes sur l'impartialité du médiateur et les difficultés que peuvent rencontrer les plaignants. Tout citoyen européen peut en effet se tourner vers la justice américaine, mais, comme le souligne le G29, ce mécanisme pourrait s'avérer trop complexe, notamment lorsqu'ils ne sont pas anglophones. L'accord doit être révisé chaque année. Lors de sa participation à sa réévaluation, le G29 « cherchera à savoir si les problèmes soulevés à l'égard du texte ont été résolus, mais aussi à déterminer si les garde-fous mis en place par le texte sont fonctionnels et effectifs ».

Quoi qu'il en soit, on notera que la démarche isolée d'un homme de 27 ans, s'engageant dans la brèche ouverte par les révélations d'Edward Snowden, remet en cause tout un dispositif engageant 29 États. Une démonstration supplémentaire de l'extraordinaire pouvoir asymétrique qu'ont les particuliers dans l'espace numérique.

[1] Accord passé le 28 juin 2010 entre l'UE et les États-Unis permettant à ces derniers d'accéder aux données bancaires des européens stockées sur le réseau de la Society for Worldwide Interbank Financial Telecommunication.

[2] Le transfert est expressément accepté par la personne concernée ou répond à des conditions énumérées par l'article 69 l'isavegarde de la vie de la personne, d'un intérêt public, exercice ou défense d'un droit en justice, etc.)

[3] Cette loi permet aux européens d'engager des actions civiles aux États-Unis en cas de violation des règles relatives à leurs données à caractère personnel.

Merci mon Général pour votre clarté ! (Denis JACOPINI)

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 la 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>



Denis JACOPINI est expert informatique spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, spyware, phishing, fraude, usurpation d'identité...) et juridiques (investigation numérique, règles RGPD, e-crime, contentieux électroniques de droit civil...)
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Fondateur de CIL (Correspondant Informatique et Libertés) ;
- Accompagnement à la mise en conformité ODL (Obligation de Légalité Obligation de Légalité)



Le Net Expert
INFORMATIQUE
Expertise et Conseil

Contactez nous

Régistrez à cet article

Original de l'article mis en page : L'accord Privacy Shield entre en vigueur [par le Général d'armée (2S) Marc Watin-Augouard, Fondateur du FIC et Directeur du CRE0GN] | Observatoire FIC

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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

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 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]

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 la 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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

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