

Le nombre de serveurs MongoDB infectés augmente chaque jour...

	Le nombre de serveurs MongoDB infectés augmente chaque jour...
---	---

L'irruption d'un groupe de cybercriminels spécialisé dans le ransomware a encore dopé le nombre de piratages des bases MongoDB. Une quinzaine d'acteurs malveillants exploitent désormais le filon.

Déjà en nette expansion la semaine dernière, l'infection touchant les bases de données MongoDB laissées librement accessibles sur Internet tourne à l'épidémie. Alors que les deux chercheurs suivant cette attaque, Victor Gevers et Niall Merrigan, recensaient un peu plus de 10 000 serveurs pris en otage vendredi, le total dépasse désormais les 28 300. Cette soudaine inflation est en grande partie due à l'entrée d'une scène d'un groupe de cybercriminels spécialistes des ransomwares, Kraken. Ce dernier, responsable à lui seul de 16 000 infections, serait entré en lice vendredi dernier, après avoir probablement pris conscience de la simplicité d'exploitation de ce nouveau filon. Selon les éléments recensés par Victor Gevers et Niall Merrigan dans un tableau récapitulant les données relatives à la quinzaine de groupes impliqués dans des attaques de ce type, Kraken aurait déjà convaincu 67 organisations de lui verser une rançon de 0,1 Bitcoin (86 euros environ) ou, dans certains cas, de 1 Bitcoin.

Rappelons que l'attaque ne consiste pas à déployer un ransomware, mais exploite la (très discutable) configuration par défaut des bases MongoDB, au sein duquel l'accès n'est pas protégé par une authentification. Lorsque que ces bases sont librement accessibles sur Internet, les pirates se contentent d'exporter le contenu des bases non sécurisées, d'effacer les données du réceptacle originel et d'y déposer un fichier comportant les informations poussant à la victime à payer une rançon (entre 0,1 et 1 Bitcoin) afin de retrouver ses données. Notons que MongoDB a publié un billet de blog expliquant comment paramétrer sa solution pour éviter ce type de mésaventure.

Un défaut connu de longue date

Victor Gevers et Niall Merrigan signalent que certains groupes de cybercriminels se contentent d'effacer les données, sans les télécharger au préalable, rendant toute récupération de l'information illusoire pour les victimes. Selon Victor Gevers, 12 organisations ayant versé une rançon à Kraken n'ont pour l'instant obtenu aucune réponse du groupe de cybercriminels. Les deux chercheurs notent également que certains acteurs malveillants en concurrence sur ce segment n'hésitent pas à remplacer les fichiers de demande de rançon d'autres groupes de hackers. La conséquence ? Les victimes peuvent se retrouver à verser des bitcoins à des individus qui, de toute façon, ne détiennent pas leurs données...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRETF n°93 84 03041 84)
- 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 : Epidémie pour MongoDB : 28 000 serveurs pris en otage

Cyberviolence: Comment sont contrôlés les groupes secrets sur Facebook ?



Cyberviolence:
Comment sont
contrôlés les
groupes secrets
sur Facebook ?

Deux groupes ont été fermés pour avoir diffusé des photos volées de femmes nues...

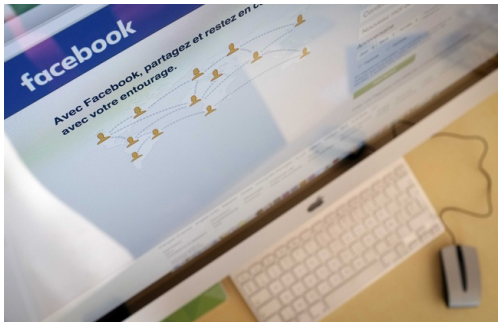


Illustration Facebook – LODI FRANCK/SIPA

Ils partageaient des photos de leurs copines nues assorties de commentaires graveleux ou insultants. Deux groupes secrets sur Facebook, « Babylone 2.0 » et « Garde ta pêche », ont été fermés en fin de semaine dernière après leur découverte par une journaliste belge. Pour pouvoir entrer dans ces groupes, il faut être coopté et personne d'autre que leurs membres ne peuvent en voir le contenu. Ce qui pose un problème au réseau social, dont le principe de modération est basé sur les signalements des utilisateurs.

« Banalisation de la violence »

« Chaque utilisateur a la possibilité de signaler tout contenu qu'il considère choquant, qu'il s'agisse d'un commentaire, d'un post, d'une page, d'un profil, etc. (...) Dès le premier signalement, le contenu est consulté et analysé par une équipe dédiée mobilisée 24 heures sur 24, 7 jours sur 7. Pour la France, nous disposons d'une équipe francophone », indique Facebook France. Il s'agit donc d'une modération *a posteriori*, qui n'intervient que lorsqu'un utilisateur du réseau alerte Facebook. Si tous les membres d'un groupe sont d'accord pour partager des contenus qui enfreignent « les standards de la communauté », il y a donc peu de chances pour que ceux-ci soient interdits.

« On sait que Facebook a des soucis de modération, estime Hélène Dupont, conseillère éditoriale sur le programme Internet sans crainte. On ne peut pas attendre de Facebook d'avoir la même vigilance qu'un média car ils n'ont pas de rédaction ou de comité éditorial. C'est pour cela que nous sommes favorables à l'éducation des utilisateurs en amont. » Chez les jeunes notamment, la connaissance des outils de signalement est importante. Mais lorsqu'ils voient un contenu qui les choque, ce n'est pas leur compétence technique qui fait défaut pour lancer une alerte : « On a vu que pour la cyberviolence ou le harcèlement, la tolérance est bien plus grande en ligne que dans la réalité, note Hélène Dupont. Il y a une banalisation de la violence sur Facebook et les jeunes en réfèrent peu à des adultes. »...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRETF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Original de l'article mis en page : Cyberviolence: Comment sont contrôlés les groupes secrets sur Facebook

13,7 millions de Français ont

été confrontées à la cybercriminalité en 2016

 Denis JACOPINI UNE CARTE BANCAIRE ANTI-FRAUDE ? Qui pourra l'identifier ? vous informe LCI	13,7 millions de Français ont été confrontés à la cybercriminalité en 2016
--	---

La nouvelle édition du rapport Norton sur les cyber risques montre le laxisme des utilisateurs français quant à leur sécurité en ligne tandis que les cyber-attaquants ne cessent de développer leurs compétences et la sophistication de leurs attaques.

France vs Monde		
		
TOP FINDINGS	FRANCE	GLOBAL (21 pays)
Individus confrontés à la cybercriminalité au cours de l'année écoulée	13,7 millions (24 %)	689,4 millions (31 %)
Coût financier total lié à la cybercriminalité au cours de l'année écoulée	1,789 milliards d'euros	125,9 milliards de dollars (soit environ 117 milliards d'euros)
Temps moyen passé à gérer les conséquences d'un acte de criminalité en ligne	9,6 heures	15,7 heures
Profil d'individus les plus touchés par la cybercriminalité au cours de l'année écoulée	Voyageurs fréquents : 31 % Millennials : 29 % Parents : 26 %	Voyageurs fréquents : 40 % Millennials : 40 % Parents : 40 %
Personnes ne sachant pas identifier un e-mail de phishing ou évaluer la validité d'un e-mail	31 %	41 %
Victimes d'un acte de cybercrime après avoir répondu à un potentiel e-mail de phishing	90 %	80 %
Individus essayant de savoir déterminer si le réseau Wi-Fi utilisé est sécurisé	56 %	48 %
Individus se sentant déçus par la quantité d'informations dont ils ont besoin pour se protéger en ligne au quotidien	33 %	39 %
Individus estimant que les appareils domestiques connectés offrent aux pirates de nouvelles façons de voler des données	81 %	72 %
Individus n'utilisant des mots de passe sécurisés que lorsqu'ils sont requis	26 %	42 %
Individus possédant au moins un terminal non protégé	35 %	35 %

En France, 13,7 millions de personnes ont été confrontées à la cybercriminalité en 2016

Norton by Symantec, a publié les résultats de son rapport annuel sur les cyber risques : au cours de l'année écoulée, 13,7 millions de Français ont été victimes d'actes de cybercriminalité. Les attaquants continuent de profiter d'un manque de vigilance de la part des utilisateurs. Le rapport montre que le coût financier lié au cyber crime s'élève à près d' 1,8 milliard d'euros en France (environ 117 milliard d'euros au niveau mondial). Quant au « coût temps », les Français victimes d'acte de cyber crime passent en moyenne 9,6 heures à en gérer les conséquences.

L'enquête, réalisée auprès d'un échantillon représentatif de 20 907 personnes répartis dans 21 pays, dont 1 008 Français, illustre l'impact de la cybercriminalité et révèle qu'alors que la prise de conscience commence à s'intensifier, de nombreuses personnes restent trop laxistes quant à la protection de leurs informations personnelles. Plus des trois-quarts des Français (77 %) savent qu'ils doivent activement protéger leurs informations en ligne, mais sont toujours enclins à cliquer sur des liens ou à ouvrir des pièces jointes douteuses provenant d'expéditeurs inconnus.

Les catégories les plus affectées par le cybercrime sont les 18-34 ans – 29% d'entre eux en ont été victimes l'an passé. Par ailleurs, 31% des voyageurs fréquents, 26% des parents et 21% des hommes ont reconnu avoir été concernés par le sujet au cours de l'année passée.

Si les comportements qui ne respectent pas les règles élémentaires de sécurité en ligne sont mis en évidence par le rapport, 81% des Français savent reconnaître un email de phishing, ce qui les place au premier rang européen et mondial. Ce score élevé résulte probablement des efforts de pédagogie des institutions gouvernementales et financières sur le sujet.

« La conclusion de notre rapport 2016 est sans appel : les internautes ont de plus en plus conscience qu'il est indispensable de protéger leurs informations personnelles en ligne mais n'ont pas envie de prendre les précautions adéquates pour assurer leur sécurité », déclare **Laurent Heslault**, expert en cyber-sécurité Norton by Symantec. « La paresse des utilisateurs n'évolue pas, mais dans le même temps, les cyber-attaquants affinent leurs compétences et adaptent leurs fraudes pour profiter davantage des internautes. Le besoin d'éducation n'a jamais été aussi fort et il est donc crucial de prendre des mesures appropriées. »

Les internautes savent que le risque est réel

La cybercriminalité est aujourd'hui si courante et répandue que les internautes la considèrent comme un risque équivalent à ceux du monde réel :

- Près de la moitié des internautes (46 %) déclare qu'il est devenu plus difficile d'assurer sa sécurité en ligne que dans le monde physique et réel ;
- Presque la moitié (47 %) estime que saisir ses informations financières sur Internet, en étant connecté à un réseau Wi-Fi public, serait plus risqué que de lire à voix haute son numéro de carte dans un lieu public ;
- Un Français sur 2 pense qu'il est plus probable que quelqu'un accède frauduleusement à leurs appareils domestiques connectés plutôt qu'à leur logement.

Et les risques sont bien réels

Les actes de cybercriminalité les plus fréquents en France sont le vol de mot de passe (14 %) et la fraude à la carte de crédit (10 %). Les deux reflètent un besoin encore présent de sensibilisation du public sur la sécurité en ligne ; en effet :

- Les Français ne vérifient pas toujours le niveau de sécurité des sites Web lors de leurs achats en ligne ;
- 1 Français sur 5 partage ses mots de passe ;
- Près d'1 Français sur 2 utilise le même sur plusieurs plates-formes et comptes.

Parmi les autres actes de cybercriminalité, le rapport sur les cyber risques Norton by Symantec a identifié le piratage électronique (11 %) et le piratage des réseaux sociaux (9 %). Alors que le ransomware représentait seulement 4 % des actes de cybercriminalité, soit environ 548 000 au cours de l'année passée ; 30 % des victimes de ransomware ont payé la rançon et 41 % ne pouvaient plus accéder à leurs fichiers.

Les mauvaises habitudes en ligne ont la vie dure

La cybercriminalité est un risque intrinsèque à notre monde connecté, mais les utilisateurs manquent toujours de vigilance et manifestent des habitudes en ligne risquées lorsqu'il s'agit de protéger leurs informations personnelles en ligne. Parmi les faits marquants de l'étude Norton by Symantec :

- L'email, ce fléau – 65 % des Français ont ouvert une pièce jointe provenant d'un expéditeur inconnu, mais seulement 35 % d'entre eux ont ouvert la porte à un étranger : il existe donc une dichotomie des comportements de sécurité entre le monde physique et le monde virtuel. Par ailleurs, 19% ne savent toujours pas identifier un email de phishing.
- Le gap générationnel – La génération Y montre des habitudes étonnamment peu sérieuses en ligne et partage facilement ses mots de passe, mettant ainsi en danger sa sécurité en ligne (35 %). C'est probablement pour cette raison que les jeunes restent les victimes les plus fréquentes puisque 29 % des Français de la génération Y ont été victimes de cybercriminalité l'année dernière ;
- La faille du mot de passe – Même si une majorité des utilisateurs (58 %) affirme utiliser un mot de passe sécurisé sur chaque compte, quasiment un internaute sur 5 (20 %) partage ses mots de passe avec d'autres personnes et nombre d'entre eux (42 %) ne voient pas le danger d'utiliser les mêmes mots de passe sur plusieurs comptes ;
- Le manque de protection – 35 % des Français ont au moins un appareil non protégé, ce qui les rend vulnérables face aux ransomware et phishing, aux sites malveillants et aux attaques zero-day. Parmi eux, 1 tiers (31 %) l'explique par le fait qu'il ne pense pas que l'appareil ait besoin d'être protégé et 27 % affirment ne rien faire de « risqué » en ligne, les rendant vulnérables à une attaque ;

Une connexion permanente à quel prix ? – L'envie de rester connecté en permanence fait que 25 % des Français préféreraient installer un programme tiers pour accéder à un Wi-Fi public plutôt que de s'en passer...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DCTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité ONIL de votre établissement.



Le Net Expert
INFORMATIQUE
Cybersécurité & Conformité

Contactez-nous



Réagissez à cet article

Original de l'article mis en page : En France, 13,7 millions de personnes ont été confrontées à la cybercriminalité en 2016
– No Web Agency

Crainte de cyberattaques lors les élections présidentielles Françaises



R

Crainte de
cyberattaques
lors les
élections
présidentielles
Françaises

Jean-Yves Le Drian a annoncé que 24.000 cybertattaques ont été déjouées en 2016, renforçant les craintes à quelques mois de la présidentielle.

La menace liée aux cyberattaques inquiète les pays occidentaux. Jean-Yves Le Drian a annoncé dans un entretien au *Journal du Dimanche* que 24.000 cybertattaques ont été déjouées en 2016, quelques jours après un rapport des services de renseignement américains pointant du doigt l'ingérence russe dans l'élection présidentielle américaine.

De quoi faire craindre des opérations similaires lors de la prochaine présidentielle en France, en avril et en mai prochain. « Il existe un risque à prendre très au sérieux que l'élection présidentielle soit menacée d'instrumentalisation par le biais d'attaques ou de propagande cyber », met en garde François Clémenceau, journaliste au *Journal du Dimanche* et auteur de l'interview.

« Les politiques ont pris des mauvaises habitudes. »

« Notre enquête auprès des formations politiques montre que la prise de conscience existe, mais elle est encore faible. Les personnalités politiques ont pris de très mauvaises habitudes dans l'utilisation de leurs téléphones et de leurs ordinateurs », s'inquiète-t-il.

Un risque d'attaque russe.

François Clémenceau affirme également que la France pourrait être victime d'une cyberattaque de la part de la Russie. « Ce qui est sûr, c'est que la France, comme l'Allemagne ou l'Italie, a une position vis-à-vis de la Russie sur l'Ukraine ou sur la Syrie... Il y a donc un intérêt du point de vue russe à déstabiliser une partie des démocraties occidentales, notamment en Europe et singulièrement la France, qui a pris des positions très dures par le biais de sanctions contre la Russie. »

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- 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 : Cyberattaque : « un risque d'instrumentalisation » de l'élection présidentielle

Combien valent vraiment vos données personnelles sur les réseaux sociaux ?



Une extension pour navigateur développée par des chercheurs de l'université de Madrid vous permet de connaître en temps réel les revenus publicitaires générés par votre profil Facebook.



Sur Internet, comme le dit l'adage : si c'est gratuit, c'est vous le produit. SUPERSTOCK/SUPERSTOCK/SIPA

MONÉTISATION. Dans le monde des *big data*, combien valent vraiment vos données personnelles sur Facebook ? Les recettes publicitaires du réseau social ne cessent de croître de façon exponentielle : 17 milliards de dollars pour 2015, contre 764 millions en 2009. Et combien d'euros gagnés grâce à votre propre activité ? Pour l'utilisateur, il est souvent délicat de répondre à cette question, tant l'opacité sur les algorithmes utilisés par les plateformes (dont réseaux sociaux) est grande. Mais une extension gratuite pour le navigateur Chrome (bientôt disponible aussi pour Opera et Firefox) développée par des chercheurs de l'université de Madrid permet d'estimer en temps réel la valeur économique dégagée par votre profil au fur et à mesure du temps passé sur le site de Mark Zuckerberg... un travail de recherche qui interroge d'ailleurs la valeur commerciale globale de nos données et les modes de régulation possibles.

Même sans cliquer sur les pubs, un internaute rapporte

L'outil madrilène, baptisé FDVT (pour Facebook Data Visualisation Tools), permet de quantifier l'évolution de la valeur publicitaire d'un profil en fonction du temps passé sur le réseau social. Il s'appuie sur le projet TYPES, financé par l'Europe dans le cadre de l'initiative Horizon 2020, qui se préoccupe de la transparence de la publicité en ligne dans l'économie numérique. « Chacun a une valeur différente sur le marché selon son profil, de sorte que l'outil ne fournit qu'une estimation des profits », expliquent Ángel et Rubén Cuevas, professeurs à l'université Charles III de Madrid et créateurs de l'extension. « Lorsque vous vous connectez à Facebook et recevez une publicité, nous déterminons la valeur qui lui est associée, le prix que ces annonceurs paient pour afficher ces publicités et chacun de vos clics sur une de ces publicités. » Les deux chercheurs ont notamment constaté que le coût d'un utilisateur américain est à peu près deux fois supérieur à celui d'un utilisateur espagnol. Et ce n'est pas tout : ils ont également mis en évidence que même sans jamais cliquer sur un lien sponsorisé, Facebook générerait néanmoins de la valeur à partir de votre profil.



Capture d'écran de l'extension : après quelques minutes seulement d'activité et sans cliquer sur aucune pub, l'auteur de ces lignes a déjà cédé près d'un dollar de revenu publicitaire à Facebook.

Une commodité marchande comme les autres ?

À l'heure où les données personnelles s'échangent pour une poignée de dollars (et notamment en Chine, on l'on peut acquérir les données personnelles de citoyens américains pour à peine 100 dollars), se pose la question de leur valorisation. Un rapport écrit fin 2016 par le Oxford Internet Institute s'interrogeait ainsi sur la chaîne de valeur des données personnelles (c'est à dire, l'évolution de leur valeur de leur création à leur utilisation dans l'économie numérique), et sur les types de régulation possibles, par exemple via une possible taxation de l'usage des données personnelles. Une démarche qui n'aurait rien d'évident, au vu de la nature internationale et dématérialisée des échanges de données...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybersécurité ; (Auteur de la certification n°10 04 0341 84)
- Formation de CIL (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Original de l'article mis en page : Sur les réseaux sociaux, combien valent vraiment vos données personnelles ? – Sciencesetavenir.fr

Dans l'armée, des aigles royaux pour lutter contre les

drones



Des soldats d'un nouveau genre... A l'occasion de ses vœux aux Armées, vendredi, François Hollande a pu se glisser dans la peau d'un dresseur d'aigles. Depuis le mois de septembre, ces rapaces sont en effet utilisés par l'Armée de l'Air pour lutter contre les drones....[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (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

Parapluie, pommeau de douche et diffuseur d'odeurs... Ces objets connectés pour faciliter le quotidien



Des odeurs pour nous aider à mieux dormir, un parapluie connecté ou encore un pommeau de douche pensé pour responsabiliser son utilisateurs sur sa consommation d'eau.....[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (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

Dans l'armée, des aigles royaux pour lutter contre les drones



Des soldats d'un nouveau genre... A l'occasion de ses vœux aux Armées, vendredi, François Hollande a pu se glisser dans la peau d'un dresseur d'aigles. Depuis le mois de septembre, ces rapaces sont en effet utilisés par l'Armée de l'Air pour lutter contre les drones....[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (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

Agir contre les rançongiciels chiffnants !

NO MORE RANSOM!

www.nomoreransom.org

**Agir contre
les
rançongiciels
chiffnants !**

Le CECyF a rejoint en décembre 2016 avec enthousiasme le programme NoMoreRansom. Il regroupe, sous l'égide d'Europol, un certain nombre de partenaires publics et privés œuvrant dans la lutte contre les cryptolockers ou rançongiciels chiffants.

Ainsi, sur le site NoMoreRansom vous trouverez des informations sur cette menace, la façon de s'en prémunir et surtout, **dès qu'une solution existe, des liens vers les outils vous permettant de déchiffrer les fichiers compromis** par le cryptolocker dont vous êtes victime...[lire la suite

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

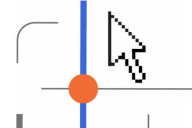


[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : No More Ransom – Agissons contre les rançongiciels chiffants ! | CECyF

Le recours au vote électronique en entreprise enfin facilité !

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LENETEXPERT.fr	 LE NET EXPERT MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
					Le recours au vote électronique en entreprise enfin facilité !

L'employeur peut maintenant décider de mettre en œuvre le vote électronique pour les élections professionnelles même en l'absence d'accord d'entreprise.

Jusqu'à présent, le recours au vote électronique pour le déroulement des élections professionnelles (délégués du personnel, membres du comité d'entreprise...) était subordonné à la conclusion d'un accord d'entreprise. Autrement dit, l'employeur n'avait pas la possibilité, en l'absence d'accord collectif, de mettre en place un tel dispositif. Une possibilité aujourd'hui offerte par la loi Travail du 8 août 2016 et dont les modalités d'application ont été fixées par décret.

Ainsi, les employeurs d'au moins 11 salariés peuvent désormais, en l'absence d'accord le prévoyant, recourir au vote électronique pour organiser les élections professionnelles au sein de l'entreprise. Attention : le décret ne précise pas si, avant de prendre une telle décision, l'employeur doit préalablement tenter de conclure un accord avec les syndicats représentatifs. Aussi lui est-il conseillé d'ouvrir de telles négociations compte tenu du risque d'annulation du scrutin qui pourrait en découler.

Il appartient alors à l'employeur de fixer les modalités du déroulement du scrutin dans un cahier des charges respectant les règles légales relatives au vote électronique. Parmi ces règles, on peut citer notamment l'obligation d'assurer la confidentialité des données transmises et la sécurité de l'adressage des moyens d'authentification ainsi que le scellement du système de vote à l'ouverture et à la clôture du scrutin. Important : le cahier des charges doit être tenu à la disposition des salariés sur le lieu de travail et, le cas échéant, figurer sur le site Intranet de l'entreprise.

Par ailleurs, lorsqu'il décide de recourir au vote électronique, l'employeur peut exclure ou autoriser le scrutin à bulletin secret sous enveloppe. Dans ce dernier cas, l'ouverture du vote à bulletin secret doit avoir lieu après la clôture du vote électronique.

Enfin, l'employeur doit informer l'ensemble des syndicats représentatifs de salariés dans l'entreprise qu'il a bien accompli la déclaration préalable du dispositif de vote auprès de la Commission nationale de l'informatique et des libertés.

Décret n° 2016-1676 du 5 décembre 2016, JO du 6

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles

3 points à retenir pour vos élections par Vote électronique

Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique

Modalités de recours au vote électronique pour les Entreprises

L'Expert Informatique obligatoire pour valider les systèmes de vote électronique

Notre sélection d'articles sur le vote électronique

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles

3 points à retenir pour vos élections par Vote électronique

Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique

Modalités de recours au vote électronique pour les Entreprises

L'Expert Informatique obligatoire pour valider les systèmes de vote électronique

Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

**Vous souhaitez organiser des élections par voie électronique ?
Cliquez ici pour une demande de chiffrage d'Expertise**



Vos expertises seront réalisées par **Denis JACOPINI** :

- Expert en Informatique **assermenté et indépendant** ;

- **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;

- ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;

- qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solutions de vote électronique ;

- et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapports d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis-à-vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à la Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Original de l'article mis en page : Le recours au vote électronique en entreprise est facilité !, Social et RH – Les Echos Business