La Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation

	La Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation

Face à la vague d'attentats qui frappe l'Europe, la Commission européenne discute actuellement de quelques changements dans les réglementations afin de permettre aux forces de Police d'accéder aux données des utilisateurs des services de Google et Facebook, sans autorisation préalable d'un Juge.

Les vagues d'attentat et la peur ambiante sont bien souvent l'occasion pour les gouvernements de voter des lois liberticides, et ce pourrait à nouveau être le cas dans toute l'Europe. La Commission européenne réfléchit actuellement à changer les réglementations afin de permettre aux forces de police d'aller piocher des informations dans les comptes des réseaux sociaux des utilisateurs, sans accord préalable de qui que ce soit.

Concrètement, le projet évoque même la possibilité pour les policiers d'origine étrangère de consulter les données privées des profils de ces réseaux sociaux, afin notamment d'enquêter sur un touriste ou une personne d'un autre pays de l'Union européenne. Exemple : vous partez en Italie pour quelques jours et vous faites arrêter par la police locale, ces derniers pourraient alors éplucher vos profils sociaux pour tenter d'obtenir plus d'informations sur vous, et ce, sans rien demander à la France.

Actuellement, trois projets de ce type ont été proposés et soumis à étude, l'un d'entre eux pouvant être adopté d'ici la fin de l'année 2018. Une des propositions évoque la possibilité de copier les données directement depuis le Cloud de la plateforme sociale afin d'en faire une sauvegarde et éviter la disparition des données en cas d'enquête…[lire la suite]

Commentaire de Denis JACOPINI

Entre Facebook qui analyse et espionne ses membres et les OPJ (Officiers de Police Judiciaire) qui peuvent consulter les données collectées par Facebook, il n'y a qu'un pas pour que ce même type de démarche soit aussi engagée auprès de Google pour qu'on nous mette des radars automatiques sur Internet qui nous flashent dès que quelqu'un en train picoler publie une photo.

Sans plaisanter, ces projets de loi consistent à permettre à des OPJ d'accéder aux zones privées de Facebook, car vous savez que lorsque vous publiez quelque chose sur Facebook, cet ajout peut être public (tout le monde peut le consulter et le voir) ou privé et il n'y a qu'un juge qui peut forcer Facebook à communiquer le contenu privé d'un compte. Ce projet ne changera rien pour ceux qui n'ont rien à se reprocher, et pas grand chose pour ceux qui ont quelques chose à se reprocher. Les OPJ pourrons disposer plus rapidement des contenus privés pour alimenter leurs enquêtes.

Il est fort probable à l'avenir qu'un autre réseau social soit utilisé par les malfrats l'histoire de faire courrier le chat…

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 d'expertises, d'audits, de formations et de sensibilisation 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 RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle… ;
- Expertises de systèmes de vote électronique ;

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *Europe : la Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation*

Quels sont avantages à se mettre en règle avec le RGPD ?

Quels sont les avantages à se mettre en règle avec le RGPD?

Avec le Règlement Général sur la Protection des Données (RGPD/GDPR), l'UE se dote d'un cadre réglementaire détaillé pour permettre à ses citoyens de reprendre le contrôle sur leurs données numériques. Pour se mettre en conformité, les entreprises ont un travail titanesque devant elles pour ne pas risquer de lourdes amandes prévues par le texte. Quels avantages peuvent tirer les entreprises de prendre le chemin de la mise en conformité ?

Au fil des conférences que nous animons ou des réunions de sensibilisations auxquelles il nous est demandé d'intervenir, nous remarquons que la grande majorité des décideurs voient d'un très mauvais oeil l'arrive de ce RGPD (Règlement Général sur la Protection des Données).

Le contexte

A cela, Denis JACOPINI, Expert Informatique spécialisé en protection des données personnelles répond plusieurs choses :

1. Ne pensez-vous pas qu'en tant que consommateur, vous êtes en droit d'avoir l'assurance que le professionnel ou le service public à qui vous confiez vos données personnelles (adresse postale, adresse e-mail, date de naissance, n° de tel portable, numéro de carte bancaire, numéro de sécurité sociale, mot de passe pour accéder à notre compte, historique et remboursement de nos actes médicaux, empreintes digitales, vocales, iriennes, adn, photocopie de pièce d'identité ou de justificatif de domicile…) mettra tous les moyens techniques en oeuvre pour protéger votre vie privée ?

A l'heure de la communication de nos données à la vitesse de la lumières peut encore penser que toutes les données nous concernant, absolument toutes, doivent être libres d'accès ?

Ceux qui ne craignent pas les usages malveillants de ces données ?

A mon avis ce sont ceux qui ne connaissent pas les conséquences d'une usurpation d'identité, d'un vol de numéro de carte bancaire ou d'un vol de mot de passe.

2. Denis JACOPINI vous demande maintenant de vous positionner à la place du responsable de l'établissement public ou privé qui a maintenant la lourde responsabilité de conserver et protéger toutes les informations que lu ont confié des milliers voire des millions de personnes.

Maintenant, n'est-il pas normal de faire le ménage dans votre système de traitement de données et de supprimer ou d'anonymiser les données inutiles ?

Ne pensez-vous pas qu'il est important de mettre à l'abris des regards indiscrets les numéros de cartes bancaires que vous avez récupéré dans votre système informatique ou bien plus couramment sur les tickets de votre TPE ?

Ne pensez-vous pas que les SEULES données pour lesquelles pour vous TOUT est permis ce sont VOS DONNÉES (votre nom, votre prénom, votre date de naissance, vos numéros de téléphone, nos numéro de CB, vos mots de passe, les chiffres de votre comptabilité…). ous pouvez faire ce que vous voulez avec VOS données (les accrocher derrière un Sessna et les faire défiler dans le ciel si ça vous chante). Toutes les autres données, celle appartenant à d'autres personnes ne vous appartiennent pas et vous ne pouvez pas faire ce que vous voulez avec.

Toutes les autres données appartiennent à des personnes qui comptent, et cela va de sois, sur votre discrétion et votre professionnalisme pour ne pas diffuser, divulguer ou rendre accessible ces données à des tiers non autorisés ou malveillants.

3. A l'heure des gros titres quasiment quotidiens faisant état d'un usage de données volées, de la diffusion ou de la vente dans le « darknet » (sorte de marché noir de l'Internet) ou pire, dans l'Internet public de données volées à des personnes comme vous et moi, il est, selon l'avis de Denis JACOPINI urgent d'arrêter de donner à manger à ces pirates informatiques qui basent avant tout leur activité lucratives sur les erreurs et failles des utilisateurs et informaticiens négligents insensibles à la sécurité informatique ne se souciant que de la part disponibilité ou intégrité dans leur applications de la sécurité informatiques, mais ni de confidentialité et encore moins d'analyse de risque.

Les opportunités pour les établissements concernés

En entamant une démarche de mise en conformité avec la Loi Informatique et liberté I ou II, avec la Loi pour une République Numérique ou avec le RGPD (Réglement Général sur la Protection des Données), Denis JACOPINI ajoute que vous allez être amenés à corriger plusieurs failles dans les traitements de données personnelles dont votre activité administrative ou professionnelles dépend :

• En vous intéressant à la durée de conservation de vos documents, vous allez épurer vos archives contenant la plupart du temps « au cas où » la totalité de la mémoire de l'entreprise de la plus petite notre manuscrite jusqu'au dossier complet sur une entreprise ou une personne en particulier. En mettant à plat l'ensemble de vos traitements de données personnelles, vous constaterez très certainement que vous conservez des données sans y être obligé. Les détruire vous permettra non seulement de gagner de la place **(Gain de place = Gain d'argent)**, mais également de réduire vos responsabilité en sécurisant l'accès à ces données confidentielles pour la plupart **(Moins de responsabilités = moins de risque)** ;

• Concernant la confidentialité, vous allez ensuite vous rendre compte qu'à la question QUI à accès à QUOI ? il est peut être temps de faire du ménage. Entre les utilisateurs qui n'existent plus et les dossiers contenant des informations sensibles partagés sans restriction particulière, il sera probablement nécessaire de revoir sa PSSI (Politique de Sécurité des Systèmes d'Information) ; L'entreprise y tirera un avantage en matière de tranquillité et surtout cela diminuera ses responsabilités en cas de vol de données **(Moins de risques = Plus de tranquillité)** ;

• Difficile de mettre en place une telle démarche sans avoir une personne dédiée à ces fonctions. Jusqu'au 25 mais 2018 il s'appelle CIL (Correspondant Informatique et Libertés) et DPO (Data Protection Officer) ensuite. Ce soldat dédié à la protection des données n'est pas là que pour dire à son employeur ce qu'il faut faire pour rester dans les clous de la réglementation sur les données personnelles ou signaler ce qu'il ne faut pas faire.

Cette personne dédiée à temps partiel ou à temps complet à ces fonctions a pour but, par son existence et sa déclaration auprès de l'autorité compétente (la CNIL en France), de rassurer celui qui vous a confié, qui vous confie et qui vous confiera encore des données personnelles. Sachant que bientôt la quasi totalité des citoyens et consommateurs déposeront des informations auprès d'organismes ou sur des site Internet essentiellement parce qu'ils ont confiance envers le service utilisé, l'existence de cet intermédiaire entre l'autorité compétente et votre établissement sera à minima essentielle pour ne pas faire fuir les usagers de vos services **(Plus de confiance = Plus d'activité)**.

Autres avantages collatéraux

En entamant une démarche de mise en conformité avec les lois relatives à la protection des données personnelles, vous contribuez à la diminution de la cybercriminalité dans le monde. En effet, données plus protégées = données difficile à voler par les pirates du Web = moins de pirates = moins de temps perdu à traiter les prélèvements frauduleux, les usurpations d'identité et pannes informatiques.

Les démarches à accomplir recommandées par Denis JACOPINI

1. Faire un état des lieux des données personnelles soumises à la réglementation ;
2. Rechercher la présence ou non de dérogation ou d'exception relatives à votre activité ou aux données personnelles traitées ;
3. Réaliser une analyse de risque relative aux données personnelles (Denis JACOPINI a spécialement passé la certification ISO 27005 qui concerne les analyses de risques relatives aux données) ;
4. Mettre en conformité les traitements des données personnelles afin qu'ils répondent aux réglementations (Loi Informatique et Libertés / Loi pour une République Numérique / Règlement Général sur la Protection des Données RGPD) ;
5. Mettre en place un registre et porter les annotations nécessaires à l'amélioration des traitements ;
6. Suivre l'évolution de l'établissement, des traitements, des risques et mettre à jour le registre.

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.

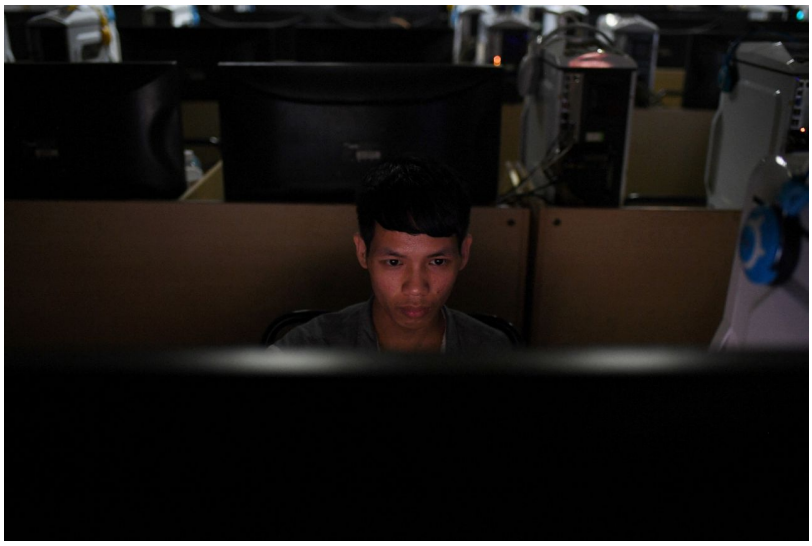
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère 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

---

Réagissez à cet article

La Chine lance sa loi sur la cybersécurité. Les entreprises sont inquiètes

	La Chine lance sa loi sur la cybersécurité. Les entreprises sont inquiètes

La Chine applique à partir de jeudi sa loi sur la cybersécurité, renforçant encore sa « Grande muraille » informatique, mais des entreprises étrangères s'inquiètent de l'impact de la nouvelle réglementation sur leurs activités.

Cette loi adoptée en novembre dernier ambitionne de protéger les réseaux chinois et les informations personnelles des utilisateurs, à l'heure où le rançongiciel WannaCry a rappelé la vulnérabilité des Etats face aux cyberattaques.
Mais des entreprises ont réclamé au gouvernement chinois un report de l'application de la loi. Elles s'inquiètent notamment des dispositions imprécises du texte et de l'influence qu'il pourrait avoir sur l'informatique dématérialisée (le « cloud ») et le traitement des données personnelles.
Les autorités semblent toutefois vouloir finaliser les règles.
Mi-mai, le directeur de l'Administration chinoise de la cybersécurité (CAC), Zhao Zeliang, a réuni 200 représentants d'entreprises et d'associations professionnelles locales et étrangères au siège de son organisme à Pékin.
La discussion était centrée sur les règles de transfert des données personnelles à l'étranger, ont rapporté des participants à l'AFP. Selon eux, les personnes présentes ont reçu une version actualisée de dispositions de la loi, et l'assurance de M. Zhao que certains des passages les plus polémiques seraient retirés.
Le nouveau document, consulté par l'AFP, ne fait par exemple plus mention de l'obligation controversée pour les entreprises de conserver en Chine les données personnelles de leurs clients.
Mais les appréhensions demeurent.
Les autorités « ne sont pas prêtes » à faire appliquer la loi et il est « très improbable » qu'un changement concret dans la législation intervienne dès le 1er juin, a assuré à l'AFP un participant qui a requis l'anonymat en raison de la sensibilité du dossier.
La Chine surveille déjà drastiquement l'internet, en bloquant les sites qu'elle estime politiquement sensibles, un système surnommé « la Grande muraille électronique » qui n'a toutefois pas empêché des universités et stations-services du pays d'être touchées par l'attaque planétaire du virus WannaCry.
La nouvelle loi sur la cybersécurité interdit aux internautes de publier tout contenu portant atteinte à « l'honneur national », « troublant l'ordre économique et social » ou destiné à « renverser le système socialiste », c'est-à-dire le Parti communiste au pouvoir.
Des entreprises étrangères craignent que la nouvelle loi entrave leur accès au marché chinois…[lire la suite]

Réagissez à cet article

Source : *La Chine lance sa loi sur la cybersécurité, les entreprises inquiètes – Le Parisien*

Qui a le droit d'accéder à nos données numériques après notre mort ?

Qui a le droit d'accéder à nos données numériques après notre mort ?

Faisant partir de la Loi du 7 octobre 2016 pour une République numérique
le 10 10 2016 (dite aussi Loi Lemaire), en complément d'un chapitre traitant de mesures sur l'ouverture des données publiques, d'un autre sur le principe de neutralité des réseaux et de portabilité des données, un chapitre traite de notre mort numérique ou en d'autres termes, après notre mort, qui pourra avoir accès aux données numériques qui nous appartenaient ?

La loi n° 78-17 du 6 janvier 1978 a été impactée par cette Loi pou rune république numérique.
L'article 40 est ainsi complété par un article 40-1 ainsi rédigé :
Art. 40-1 article I. : « Les droits ouverts à la présente section s'éteignent au décès de leur titulaire. Toutefois, ils peuvent être provisoirement maintenus conformément aux II et III suivants.

Art. 40-1 article II. : « Toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ces directives sont générales ou particulières.
« Les directives générales concernent l'ensemble des données à caractère personnel se rapportant à la personne concernée et peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la Commission nationale de l'informatique et des libertés.
« Les références des directives générales et le tiers de confiance auprès duquel elles sont enregistrées sont inscrites dans un registre unique dont les modalités et l'accès sont fixés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés.
« Les directives particulières concernent les traitements de données à caractère personnel mentionnées par ces directives. Elles sont enregistrées auprès des responsables de traitement concernés. Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci des conditions générales d'utilisation.
« Les directives générales et particulières définissent la manière dont la personne entend que soient exercés, après son décès, les droits mentionnés à la présente section. Le respect de ces directives est sans préjudice des dispositions applicables aux archives publiques comportant des données à caractère personnel.
« Lorsque les directives prévoient la communication de données qui comportent également des données à caractère personnel relatives à des tiers, cette communication s'effectue dans le respect de la présente loi.
« La personne peut modifier ou révoquer ses directives à tout moment.
« Les directives mentionnées au premier alinéa du présent II peuvent désigner une personne chargée de leur exécution. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés. A défaut de désignation ou, sauf directive contraire, en cas de décès de la personne désignée, ses héritiers ont qualité pour prendre connaissance des directives au décès de leur auteur et demander leur mise en œuvre aux responsables de traitement concernés.
« Toute clause contractuelle des conditions générales d'utilisation d'un traitement portant sur des données à caractère personnel limitant les prérogatives reconnues à la personne en vertu du présent article est réputée non écrite.

Art. 40-1 article IIII.-En l'absence de directives ou de mention contraire dans lesdites directives, les héritiers de la personne concernée peuvent exercer après son décès les droits mentionnés à la présente section dans la mesure nécessaire :
• «-à l'organisation et au règlement de la succession du défunt. A ce titre, les héritiers peuvent accéder aux traitements de données à caractère personnel qui le concernent afin d'identifier et d'obtenir communication des informations utiles à la liquidation et au partage de la succession. Ils peuvent aussi recevoir communication des biens numériques ou des données s'apparentant à des souvenirs de famille, transmissibles aux héritiers ;
• «-à la prise en compte, par les responsables de traitement, de son décès. A ce titre, les héritiers peuvent faire procéder à la clôture des comptes utilisateurs du défunt, s'opposer à la poursuite des traitements de données à caractère personnel le concernant ou faire procéder à leur mise à jour.
« Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en application du troisième alinéa du présent III.
« Les désaccords entre héritiers sur l'exercice des droits prévus au présent III sont portés devant le tribunal de grande instance compétent.
« IV.-Tout prestataire d'un service de communication au public en ligne informe l'utilisateur du sort des données qui le concernent à son décès et lui permet de choisir de communiquer ou non ses données à un tiers qu'il désigne. » ;

Source : *LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique | Legifrance*

Chrome Flaw Allows Sites to

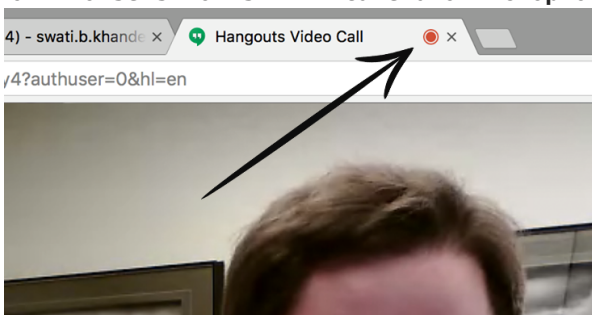
Secretly Record Audio/Video Without Indication

Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication

Sounds really scary! Isn't it? But this scenario is not only possible but is hell easy to accomplish.A UX design flaw in the Google's Chrome browser could allow malicious websites to record audio or video without alerting the user or giving any visual indication that the user is being spied on.

AOL developer Ran Bar-Zik reported the vulnerability to Google on April 10, 2017, but the tech giant declined to consider this vulnerability a valid security issue, which means that there is no official patch on the way.

How Browsers Works With Camera & Microphone



Before jumping onto vulnerability details, you first need to know that web browser based audio-video communication relies on WebRTC (Web Real-Time Communications) protocol – a collection of communications protocols that is being supported by most modern web browsers to enable real-time communication over peer-to-peer connections without the use of plugins.

However, to protect unauthorised streaming of audio and video without user's permission, the web browser first request users to explicitly allow websites to use WebRTC and access device camera/microphone.

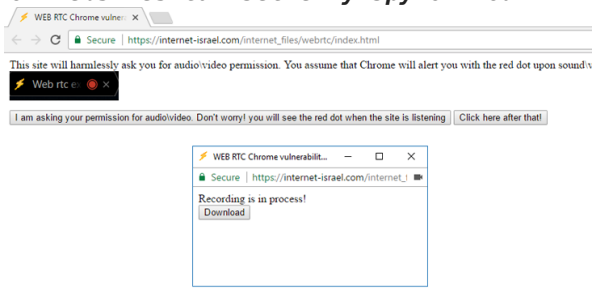
Once granted, the website will have access to your camera and microphone forever until you manually revoke WebRTC permissions.

In order to prevent 'authorised' websites from secretly recording your audio or video stream, web browsers indicate their users when any audio or video is being recorded.

« Activating this API will alert the user that the audio or video from one of the devices is being captured, » Bar-Zik wrote on a Medium blog post. « This record indication is the last and the most important line of defense. »

In the case of Google Chrome, a red dot icon appears on the tab, alerting users that the audio or video streaming is live.

How Websites Can Secretly Spy On You



The researcher discovered that if any authorised website pop-ups a headless window using a JavaScript code, it can start recording audio and video secretly, without the red dot icon, giving no indications in the browser that the streaming is happening…[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 d'expertises, d'audits, de formations et de sensibilisation 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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication*

Les PME , dépassées par l’arrivée du RGPD ?

Les PME , dépassées par l’arrivée du RGPD ?

Le Règlement Général sur la Protection des Données (GDPR) dont sa application est déjà prévue pour le 25 mai 2018, laisse aux entreprises un peu plus d'une année pour se conformer. Cependant, elles semblent toutefois avoir du mal à lancer les projets adaptés pour assurer leur conformité à ce nouveau Règlement.

Au moins c'est la conclusion principale du dernier rapport mené par IDC selon lequel **Sur les 700 entreprises interrogées, 77% des décideurs informatiques ne sont pas conscients de l'impact du RGPD sur l'activité de leur entreprise ou n'ont même pas connaissance de ce règlement.** Parmi celles qui connaissent le RGPD, 20% affirment y être déjà conformes, 59% travaillent à l'être et 21% avouent ne pas du tout être préparés.
« La protection des données à caractère personnel des clients et partenaires est primordiale pour les entreprises. Elles doivent prendre conscience de la valeur que représentent ces informations et mettre en place des mesures adaptées pour répondre aux obligations du RGPD. », explique Mark CHILD, Research Manager chez IDC. Dans ce sens, **les petites et moyennes entreprises reconnaissent que leur logiciel anti-malware est insuffisant dans l'environnement de menace actuel**, et la moitié des répondants ont avoué que ce point était le plus important à améliorer…[lire la suite]

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner 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 ».

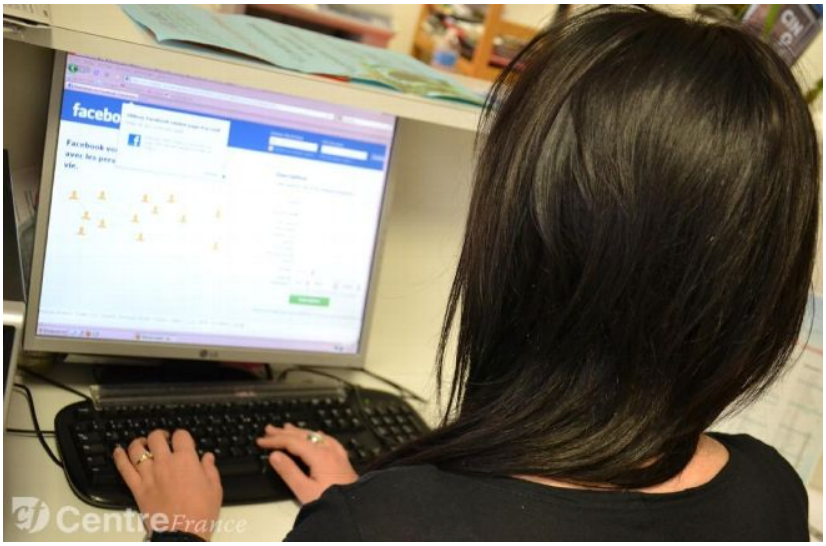
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation 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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Les PME , dépassées par l'arrivée du RGPD ? – Globb Security FR*

Conférence-débat sur la cybercriminalité. Quels dangers, quelle prévention ? Entrée gratuite.



Conférence-débat sur la cybercriminalité. Quels dangers, quelle prévention ? Entrée gratuite.

La médiathèque de Roanne propose, le samedi 13 mai prochain, une conférence-débat sur le thème « Cybercriminalité : déjouer les pièges ». Ce sera une immersion en 1 h 30 dans les méandres de la toile.

Comme chaque trimestre, la médiathèque de Roanne organise une conférence-débat pour aborder des thématiques liées au multimédia et à internet, le samedi 13 mai, de 15 heures à 16 h 30, avec pour sujet « Cybercriminalité : déjouer les pièges » ou « Comment profiter d'internet en toute sécurité ».

Autour d'une présentation très interactive, cette conférence-débat permettra de répondre aux nombreuses questions que peuvent se poser les utilisateurs du web.

Escroqueries, dérives et esquives

Sécurité et risques sur le net, messagerie, mobilité, arnaques en tous genres, prévention, vocabulaire et procédures, pratiques des jeunes, légalité ou pas dans le streaming, virus, mots de passe sécurisés… seront les notions abordées au fil de cet atelier ouvert à tous.

« C'est une formule qui est assez bien reçue et qui plait au public. La conférence-débat se veut très interactive et ouverte », annonce Franck Guigue, responsable des espaces des pratiques numériques à la mairie de Roanne, qui sera l'animateur de cette rencontre. Elle sera aussi l'occasion pour les internautes de faire le point sur les escroqueries les plus fréquemment rencontrées et donner les clés aux utilisateurs du web pour esquiver les nombreux attrape-nigauds.

Pratique. Samedi 13 mai, de 15 heures à 16 h 30, à la médiathèque de Roanne, avenue de Paris. Conférence ouverte à tout public. Entrée libre. Renseignements sur le site internet : www.bm-roanne.fr

---

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 d'expertises, d'audits, de formations et de sensibilisation 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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *La cybercriminalité : quels dangers, quelle prévention ? – Roanne (42300) – Le Pays*

Le hacker du mouvement En Marche serait identifié

Le hacker du mouvement En Marche serait identifié

Une source de Sciences et Avenir divulgue le pseudo du hacker qui serait responsable de la cyberattaque visant l'équipe de En Marche ! le mouvement d'Emmanuel Macron, élu ce soir nouveau Président de la république.

C'est à partir d'un serveur en Allemagne que serait venue la cyberattaque mettant en ligne 9 gigaoctets de documents du mouvement En Marche !, nous a révélé une ingénieure en informatique, Seraya Maouche, qui a géré un compte de campagne du nouveau président de la République Emmanuel Macron. Et le pseudo (du moins peut-on l'imaginer) du hacker s'intitule » franckmacher1 « , comme le montre la copie d'écran qui nous a été communiquée, éléments également transférés à l'équipe digitale du mouvement, nous a-t-elle assuré. Rappelons que ce hacking organisé, l'affaire étant désormais rebaptisée #Macronleaks, a pris corps sur les réseaux sociaux vendredi 5 mai 2017 au soir, vers 20H, alors que Emmanuel Macron répondait à une émission en direct sur le site de Mediapart. Et hier, samedi, la commission de contrôle de la campagne électorale pour la présidentielle française a appelé les médias à s'abstenir de relayer les documents frauduleusement obtenus.


```
<metadata>
  <identifier>Macron_201705</identifier>
  <mediatype>texts</mediatype>
  <collection>opensource</collection>
  <description>Mail archive</description>
  <scanner>Internet Archive HTML5
  Uploader 1.6.3</scanner>
  <subject>Macron</subject>
  <title>Macron</title>
  <publicdate>2017-05-05
  11:17:39</publicdate>
  <uploader>frankmacher1@gmx.de</uploader
  >
  <addeddate>2017-05-05
  11:17:39</addeddate>
   <curation>
    [curator]validator@archive.org[/curat
    or][date]20170505112302[/date]
    [comment]checked for
    malware[/comment]
  </curation>
  <language>English</language>
  <identifier-
  access>http://archive.org/details/Macro
  n_201705</identifier-access>
  <identifier-
  ark>ark:/13960/t7np7fg57</identifier-
  ark>
  <repub_state>4</repub_state>
</metadata>
```


[lire la suite]

Photo © PHILIPPE HUGUEN / AFP

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 d'expertises, d'audits, de formations et de sensibilisation 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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Macronleaks : le hacker à l'origine du piratage serait identifié – Sciencesetavenir.fr*

En marche ! dénonce un piratage « massif et coordonné » de la campagne de Macron

En marche ! dénonce un piratage « massif et coordonné » de la campagne de Macron

Le mouvement fondé par l'ancien ministre de l'économie évoque une tentative de déstabilisation de l'élection présidentielle française

Dans un communiqué diffusé dans la nuit du vendredi 5 mai au samedi 6, l'équipe du candidat à la présidentielle Emmanuel Macron a dénoncé une *« action de piratage massive et coordonnée »* d'informations *« internes de nature diverse (mails, documents comptables, contrats…) »* de sa campagne électorale.
Ce texte d'En marche ! a suivi la publication en ligne, plus tôt dans la soirée, de nombreux documents présentés comme des « #MacronLeaks » sur les réseaux sociaux. Les documents, au format .eml, sont apparus sous la forme de liens publiés sur le site *Pastebin*, sorte de bloc-notes public en ligne prisé des informaticiens et des groupes de hackeurs parce qu'il permet de publier des documents de manière relativement anonyme…[lire la suite]

Réagissez à cet article

Source : *En marche ! dénonce un piratage « massif et coordonné » de la campagne de Macron*

Sur la Protection des données personnelles, les programmes d’Emmanuel Macron et Marine Le Pen sont plutôt faibles

Sur la Protection des données personnelles, les programmes d’Emmanuel Macron et Marine Le Pen sont plutôt faibles

Emmanuel Macron et Marine Le Pen présentent tous les deux des programmes numériques assez parcellaires. On fait le point.

Sur la question de la vie privée des internautes, **Marine Le Pen** propose de « créer une charte à valeur constitutionnelle de protection des données personnelles », sans jamais préciser ce qu'une telle charte pourrait induire pour les citoyens. La candidate frontiste souhaite également mettre en place l'obligation « de stocker les données personnelles des Français sur des serveurs hébergés en France », sans toutefois livrer plus de détails sur les modalités techniques de telles mesures. Seule véritable proposition concrète dans ce dossier : la création de la carte unique biométrique, qu'elle aimerait étendre à la carte vitale afin de lutter contre la fraude, et l'obligation pour les entreprises de sotcker en France les données personnelles des citoyens français.

Emmanuel Macron, lui, reste tout autant vague. Il souhaite « développer les instruments d'une transparence sur l'usage des données privées par les acteurs du numérique« , mais ne dit pas lesquels. On retrouve le même flou lorsqu'il propos de « bâtir des murailles » et « patouiller dans le cyberespace » pour faire de la cybersécurité, « une priorité de la sécurité nationale ». L'ancien ministre de l'Économie et des finances va même jusqu'à proposer »une banque de données numériques réutilisables : « Dans le respect de la vie privée et du secret des affaires, les administrations qui délivrent des licences (par exemple pour les hôtels) devront mettre à disposition leurs données. Face aux géants étrangers, des nouvelles start-up pourront ainsi s'adresser par exemple à tous les hôteliers pour leur offrir une alternative aux services existants ». Et l'ancien banquier d'affaires français de suggérer également « un service public numérique de la justice », avec portail unique d'accès : « Les citoyens et leurs avocats y trouveront toutes les informations pratiques et la jurisprudence applicable à leur cas. Ils pourront se pourvoir en justice depuis leur ordinateur, transmettre une requête, des pièces, ou suivre leur dossier depuis leur smartphone ». Il aimerait également renégocier le « Privacy Shield » d'ici 2018 et créer une « agence européenne pour la confiance numérique » qui serait « chargée de réguler les grandes plateformes numériques »…[lire la suite]

Réagissez à cet article

Source : *Sur le numérique, les programmes d'Emmanuel Macron et Marine Le Pen sont plutôt faibles*