Uber : ces inquiétants témoignages de Français qui rapportent des piratages

	Uber : ces inquiétants témoignages de Français qui rapportent des piratages

La révélation fin novembre 2017 du hacking géant de Uber, qui s'est fait voler les données de 57 millions d'utilisateurs à travers le monde, a de quoi inquiéter les habitués de l'appli. Si l'entreprise assure que leurs coordonnées bancaires sont à l'abri, des Français témoignent avoir vu leur compte piraté pour des sommes parfois très conséquentes.
Un séisme dans le joyeux monde des applis. La direction d'Uber a admis cette semaine que les données de 57 millions de ses utilisateurs avaient été piratées en octobre 2016. Après avoir donc dissimulé ce hacking d'ampleur pendant un an, l'entreprise s'est empressée d'assurer ce mardi 21 novembre que les coordonnées bancaires des usagers concernés n'avaient pas été dérobées. *« Cela me paraît très bizarre qu'Uber ne stocke qu'une partie des données dans son Cloud Amazon, celui qui a été hacké par les pirates, sans les numéros de cartes bancaires»* , relève pour *Marianne* Julie Gommes, experte en cyber-sécurité. *« Que les données bancaires ne soient pas du tout concernées me semble peu probable»* , abonde Claire Juiff, experte conseil en gestion de crise et formée au cyber-risque…[lire la suite]

Source : *Uber : ces inquiétants témoignages de Français qui rapportent des piratages*

Votre télévision connectée vous espionne… même éteinte ?

Votre télévision connectée vous espionne… même éteinte ?

Dans plus de 25 % des cas, votre télévision connectée vous espionne et elle diffuse de nombreuses informations vous concernant sur Internet. Pire, vous n'avez aucune idée des informations recueillies, des personnes qui reçoivent ces données et de ce qu'elles font avec.

Une heure avec une télévision connectée

[…] il se trouve que nous achetons déjà ce genre d'appareils, et ces objets connectés en savent long sur nous. En une heure seulement, Avira a constaté qu'une smart TV fouinait et relevait une quantité d'informations sur son domicile : A ouvert trois ports vulnérables sur Internet ; à scanné le réseau du domicile pour trouver d'autres objets connectés ; à recueilli 750 pages d'informations textuelles sur la personne qui utilise l'appareil et sa façon de l'utiliser ; à envoyé ces informations à 13 serveurs, dont nombre sont inconnus ; à transféré les informations aux services non activés et n'ayant pas de compte utilisateur inscrit ; pire encore, la télévision a effectué tout cela alors que personne dans la maison ne l'utilisait activement…[lire la suite]

LE NET EXPERT

:

• **MISE EN CONFORMITÉ RGPD / CNIL**

- **AUDIT RGPD** de vos traitements

- **MISE EN CONFORMITÉ RGPD** de vos traitements

- **SUIVI** de l'évolution de vos traitements

• **FORMATIONS / SENSIBILISATION** :

- **CYBERCRIMINALITÉ**

- **PROTECTION DES DONNÉES PERSONNELLES**

- AU **RGPD**

- À LA **FONCTION DE DPO**

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)

- TÉLÉPHONES (récupération de **Photos / SMS**)

- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES

- **SÉCURITÉ** INFORMATIQUE

- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (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

Réagissez à cet article

Source : *ZATAZ Votre télévision connectée vous espionne… même éteinte ? – ZATAZ*

Une faille permet d'écouter 77 % des smartphones Android

	Une faille permet d'écouter 77 % des smartphones Android

---

Voilà qui risque d'augmenter la paranoïa de celles et ceux qui pensent qu'ils sont écoutés, via leur smartphone, à tout moment de la journée : les chercheurs de MWR Labs ont découvert une nouvelle faille majeure qui toucherait plus des trois quarts des smartphones Android en circulation. Une faille que Google a comblée, mais seulement dans Android 8.0 Oreo.

Le problème de cette nouvelle faille, c'est qu'elle est très facilement exploitable par un développeur malintentionné : il ne s'agit pas d'une attaque à proprement parler mais d'un souci dans les autorisations données aux applications.

Le service Android MediaProjection au centre de cette nouvelle faille

Les chercheurs de MWR Labs ont découvert que Google, qui développe Android, a réalisé un changement majeur dans les autorisations d'un des services les plus anciens d'Android : MediaProjection. Ce service est en mesure d'enregistrer l'audio ainsi que l'écran du smartphone et est utilisé par certaines applications….[lire la suite]

Réagissez à cet article

Source : *Une faille permet d’écouter 77 % des smartphones Android*

Uber : Les données de 57 millions d’utilisateurs ont été piratées

	**Uber : Les données de 57 millions d’utilisateurs ont été piratées**

Les noms ainsi que les adresses électroniques et numéros de téléphone ont été subtilisés, mais les données bancaires auraient été épargnées.

Le PDG d'Uber a révélé mardi que les données de 57 millions d'utilisateurs à travers le monde ont été piratées à la fin 2016. Parmi les 57 millions d'utilisateurs figurent 600 000 chauffeurs dont les noms et numéros de permis de conduire ont été récupérés. Les noms des utilisateurs ainsi que leurs adresses électroniques et numéros de téléphone mobile ont été subtilisés, a indiqué Dara Khosrowshahi, dans un communiqué.
Sur le base d'expertises externes, le patron affirme que l'historique des trajets, les numéros de cartes et de comptes bancaires, les numéros de Sécurité sociale et les dates de naissance des utilisateurs n'auraient en revanche pas été piratés.
M. Khosrowshahi, qui a été nommé à la tête d'Uber fin août, souligne qu'il a été informé « *récemment* » de cet incident. Il précise que deux personnes ne faisant pas partie de l'entreprise seraient responsables de ce piratage. « *L'incident n'a pas atteint les systèmes de l'entreprise ni son infrastructure* », ajoute-t-il par ailleurs.
Selon Bloomberg, Uber aurait payé 100 000 dollars les hackers afin qu'ils ne divulguent pas cet incident, une information qui n'a pas été confirmée par Uber…[lire la suite]

Réagissez à cet article

Source : *Uber révèle que les données de 57 millions d'utilisateurs ont été piratées*

Parents et futurs parents : Anticiper les risques du harcèlement sur Internet

Parents et futurs parents : Anticiper les risques du harcèlement sur Internet

---

Si le harcèlement est bien connu, le cyberharcèlement l'est beaucoup moins ! Le cyberharcèlement est une forme de cybercriminalité qui se caractérise par l'utilisation de la technologie pour harceler ou menacer en ligne une personne ou une entreprise.

L'assaillant s'infiltre dans les e-mails, la messagerie instantanée, les chats, les comptes de réseaux sociaux et les comptes bancaires en ligne, etc. de ses victimes pour les faire chanter.

En d'autres termes, il s'agit de harcèlement, mais dans le cyberespace.

Attention toutefois à ne pas confondre cyberharcèlement et trolling. Si le trolling désigne la participation d'un groupe ou d'une personne isolée à un acte de harcèlement en ligne, il comporte généralement une note d'humour – alors que le cyberharcèlement affiche des intentions malveillantes.

Les différents types de cyberharcèlement

• Prendre ou publier de vraies ou fausses photos à caractère sexuel de la victime ou de ses proches ;
• Suivre à la trace le moindre mouvement des victimes à l'aide d'un dispositif GPS installé sur leur véhicule ;
• Menacer la victime ou ses amis et sa famille par e-mail ;
• Mettre en ligne des informations personnelles telles que le nom, l'adresse, les numéros de sécurité sociale et de téléphone de la victime ;
• Pirater et enregistrer des e-mails, des SMS et des billets publiés sur les réseaux sociaux pour les utiliser dans le but de harceler ou de faire chanter la victime ;
• Pirater le compte de la victime sur les réseaux sociaux pour y publier des contenus et commentaires offensants ;
• Dévoiler des informations personnelles erronées dans le but de discréditer la victime sur son lieu de travail ;
• Utiliser le compte de réseau social ou l'e-mail de la victime pour harceler et contacter d'autres personnes ;
• Créer des sites Web malveillants, de faux profils sur les réseaux sociaux et des blogs bidon sur la victime…[lire la suite]

Réagissez à cet article

Source : *Le cyberharcèlement augmente chaque année : comment s'en protéger ? – Global Security Mag Online*

Alerte : Une faille de sécurité sur des jouets connectés expose les enfants

Alerte : Une faille de sécurité sur des jouets connectés expose les enfants

---

Une association de consommateurs britannique alerte sur une faille de sécurité liée à la connexion Bluetooth de certains jouets connectés et appelle à ce que ces derniers soient retirés de la vente.

Alors que certains ont déjà effectué les premiers achats de Noël, l'association britannique de consommateurs **Why ?** alerte les consommateurs sur le risque présenté par plusieurs jouets connectés : la peluche Furby Connect, le robot i-Que, le petit chien Toy-Fi Teddy et les animaux CloudPets. En cause : **une faille de sécurité** qui permet à toute personne ayant une connexion Bluetooth et ayant téléchargé l'application de ces jouets de se connecter à ces derniers, sans mot de passe ou étape de sécurité.

Une situation rendue possible par la **non-sécurisation de la connexion Bluetooth** de ces jouets, selon les tests réalisés par Why ? avec l'aide de Stiftung Warentest, l'équivalent allemand de l'UFC Que choisir…[lire la suite]

Source : *VIDÉO – Une faille de sécurité sur des jouets connectés expose les enfants*

Conseils pour protéger vos enfants du Cyberharcèlement

	**Conseils pour protéger vos enfants du Cyberharcèlement**

Le succès des nouvelles technologies auprès des jeunes mineurs implique de nouveaux défis pour les parents. Les protéger du cyberharcèlement en fait partie. Les attaques personnelles à travers les réseaux sociaux ou les applications de messagerie instantanée chez les jeunes se multiplient. Voici neuf conseils pour protéger vos enfants du cyberharcèlement.

Pour éviter que les mineurs ne soient victimes de ce genre d'agressions, il est important que les parents soient au courant des activités de leurs enfants sur internet. Comment ? En les alertant des dangers potentiels auxquels ils s'exposent et en leur montrant les bons usages des nouvelles technologies.

Rester ouverts à la discussion

Le dialogue parents/enfants doit être facilité. Cela passe par l'information, à commencer par leur expliquer les risques auxquels ils s'exposent en utilisant internet et les conséquences de leurs mauvaises actions. Aussi, les enfants ne doivent pas hésiter à partager leurs expériences en ligne avec leurs parents, leurs frères et sœurs ou d'autres adultes de confiance, notamment sur des sujets qu'ils ne maîtrisent pas encore bien, de par leur jeune âge. En tant que parents, n'hésitez pas à leur dire qu'ils peuvent vous parler de tout, surtout s'ils ont des doutes ou des craintes.

Mettre en place des règles

La mise en place de règles d'usage concernant Internet est également un moyen de protéger votre enfant du cyberharcèlement. Refuser des demandes d'amis, des offres ou des conseils envoyés par des inconnus ou provenant d'applications non officielles ou non vérifiées est la première des règles à faire appliquer. Le Centre pour l'éducation aux médias et à l'information (Clemi) a édité un guide pratique (« La Famille Tout-Ecran ») pour accompagner les parents et sensibiliser les enseignants sur les pratiques médiatiques des élèves. Le guide est téléchargeable ici.

Leur montrer comment réagir face au cyberharcèlement

En cas de cyberharcèlement ou d'autres problèmes liés à internet, l'enfant doit savoir que la première chose à faire est d'en parler à un adulte de confiance. Dites-lui aussi que les messages sont des preuves importantes et ne doivent donc pas être effacés si jamais le problème se transforme en délit et fait l'objet d'une plainte. Enfin l'enfant doit être averti qu'il ne doit pas non plus répondre au cyberharcèlement par le cyberharcèlement, dans un désir de vengeance.

Sécuriser leurs appareils

Les experts recommandent aux parents d'installer un système de contrôle parental sur tous les dispositifs électroniques ayant un accès à internet (ordinateurs et tablettes). La plupart des programmes de sécurité, comme les antivirus ou les pare-feux disposent d'une option « Contrôle Parental », un service qui permet aux adultes d'avoir la main sur l'utilisation d'internet par les mineurs et de bloquer certains contenus…[lire la suite]

Réagissez à cet article

Source : *Cyberharcèlement – Des conseils pour protéger vos enfants*

Loi renseignement : une première «boîte noire»

activée pour surveiller les communications

Loi renseignement : une première «boîte noire» activée pour surveiller les communications

Ce dispositif donne aux services de renseignement français un moyen d'analyser automatiquement les métadonnées des communications Internet, notamment pour lutter contre le terrorisme.

De nouvelles oreilles pour le renseignement. Longtemps inactives, les boîtes noires sont désormais en cours de déploiement. Francis Delon, le président de la Commission nationale de contrôle des techniques de renseignement (CNCTR), l'a révélé à l'occasion d'une conférence organisée à Grenoble. Il précise qu'une première boîte noire a été activée «début octobre», à l'issue d'un «travail qui a duré plusieurs mois».

Prévu par l'article 851-3 du Code de la sécurité intérieure, le dispositif a été particulièrement critiqué en amont du vote de la loi renseignement de 2015. Il permet aux services de renseignement d'analyser de grandes quantités de métadonnées (relatives au contexte d'un message, comme son origine ou sa date d'envoi) à la volée, afin de détecter une éventuelle menace terroriste. Francis Delon se veut néanmoins rassurant. «Les données récoltées sont des données de connexion anonymisées, recueillies de façon non ciblée pour être mises dans une sorte de grande marmite étanche», a-t-il résumé, par une métaphore de son cru…[lire la suite]

Source : *Loi renseignement : une première «boîte noire» activée pour surveiller les communications*

RGPD : les petites entreprises tout aussi concernées que les grandes

	RGPD : les petites entreprises tout aussi concernées que les grandes

Le règlement général européen sur la protection des données sera mis en œuvre le 25 mai 2018 pour améliorer la protection et la confidentialité des données et responsabiliser davantage les entreprises en développant l'auto-contrôle. Celles-ci devront dorénavant s'assurer que toutes les données qu'elles stockent sont en conformité avec la réglementation.

Le 25 mai prochain, toutes les entreprises devront se conformer à la nouvelle réglementation générale des données personnelles (RGPD). Celle-ci vise à établir des règles claires et unifiées pour que les individus puissent mieux contrôler les données qui les concernent. Les obligations visent toutes les entreprises, en B to B comme en B to C, quelle que soit leur taille, à partir du moment où elles collectent, traitent, gèrent et utilisent des données, que ce soit des fichiers collaborateurs en interne ou des données sur leurs clients ou fournisseurs. « Un ancien candidat qui a envoyé son CV à l'entreprise pour y postuler constitue par exemple une donnée collectée » cite Nathalie Rouvet Lazare, PDG de Coheris qui édite des solutions CRM et analytiques sur le sujet.

Toutes les données stockées sont concernées

Les données considérées comme personnelles sont nombreuses : nom, adresse, localisation, identifiant, date de naissance, IP…, autrement dit toutes les données qui permettent d'identifier une personne. Même si les données ne sont pas utilisées et traitées, à partir du moment où elles sont stockées au sein de l'entreprise, elles sont concernées par la réglementation. Même chose en termes de forme : tous les fichiers, du tableur Excel aux bases de données de prospects, salariés ou visiteurs d'un site Internet ou d'une boutique physique, sont visés. Nathalie Rouvet Lazare se veut rassurante : « Les petites entreprises doivent elles aussi se mettre en ordre de marche et établir une feuille de route. Il ne faut pas y voir une usine à gaz ou une contrainte de plus mais utiliser cette nouvelle réglementation comme une opportunité pour optimiser les données de l'entreprise ». Si celles-ci ont tendance à collecter un maximum de données, au final, peu d'entre elles les utilisent. « Elles devront dorénavant mener une réflexion préalable sur leur objectif pour chaque donnée collectée. »

Se conformer au règlement en 3 étapes

Pour mettre en place une gouvernance des données personnelles, les entreprises doivent commencer par :

• nommer une personne référente au sein de l'entreprise qui sera le pilote responsable de la mise en place des process et des outils. « Si les entreprises n'ont pas l'obligation légale de nommer un DPO (Data Protection Officer ou Délégué à la Protection des Données), il est essentiel de désigner un porteur de projet sur le sujet. »

• réaliser un audit, soit cartographier toutes les données personnelles et sensibles de l'entreprise, définir dans quels types de fichiers elles sont utilisées et comment elles sont gérées.

• passer au crible ses obligations et définir ses process et responsabilités pour s'assurer qu'elle est en conformité avec la loi.

L'occasion de mettre en place plusieurs bonnes pratiques pour répondre aux nouvelles obligations liées à la RGPD, comme un process pour protéger les données dès leur conception – data protection de by design–, la vérification de la protection effective de ses données, l'élimination des données récoltées de façon illicite ou déloyale, la révision de ses procédures de consentement qui doit être clair et circonstancié. Et si l'entreprise souhaite partager ses données personnelles avec ses partenaires, elle doit en préciser l'identité et la finalité du partage. C'est ce que l'on appelle la récolte opt-in. Enfin, avec la RGPD, les entreprises doivent être en mesure de respecter l'exercice du droit d'opposition, de rectification, d'accès direct, de portabilité et d'effacement des données…[lire la suite]

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD ?** ?
Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?
Contactez-nous

A Lire aussi :
Mise en conformité RGPD : Mode d'emploi
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
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 étapes
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 : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

---

Réagissez à cet article

Source : *Protection des données : les petites entreprises tout aussi concernées que les grandes*

Alerte : Hameçonnage (phishing) – Attention aux courriels frauduleux sur la carte Vitale V3 avec le logo de Service-public.fr

Alerte : Hameçonnage (phishing) – Attention aux courriels frauduleux sur la carte Vitale V3 avec le logo de Service-public.fr

---

Service-public.fr, le site officiel de l'administration française, vous met en garde contre l'envoi de courriels frauduleux se faisant passer pour Service-public.fr.

Le dernier cas signalé concerne un courriel les invitant à télécharger un formulaire pour obtenir, sous 24 heures, la nouvelle carte Vitale V3.
Ces courriels n'émanent pas de Service-public.fr.
Il s'agit vraisemblablement d'une manœuvre frauduleuse pour inciter les internautes à livrer leurs données personnelles.
N'y répondez pas et supprimez-les de votre messagerie électronique.
Si vous avez déjà communiqué vos données bancaires, prévenez votre banque pour faire opposition. Service-public.fr ne demande pas d'argent, n'en rembourse pas et ne cherche jamais à recueillir des coordonnées bancaires.
Illustration 1Crédits : © Dila

Rappel :
• Si vous recevez des messages non sollicités sur votre messagerie électronique, vous pouvez l'indiquer sur signal-spam .
• Pour signaler des contenus ou des comportements illicites sur internet, connectez-vous au site internet-signalement.gouv.fr .
…[lire la suite]

LE NET EXPERT
:
• **FORMATIONS / SENSIBILISATION** :
- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**
• **MISE EN CONFORMITÉ RGPD / CNIL**
- **ÉTAT DES LIEUX RGPD** de vos traitements)
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES
• **EXPERTISES** & **AUDITS** (certifié ISO 27005)
- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous
Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Réagissez à cet article

Source : *Hameçonnage (phishing) -Attention aux courriels frauduleux sur la carte Vitale V3 avec le logo de Service-public.fr | service-public.fr*