Les géants du web s’accordent pour bloquer les contenus illégaux

Les géants du web ensemble pour bloquer les contenus illégaux

Alors que les propos haineux sont malheureusement légion sur les réseaux sociaux, plusieurs géants du web ont trouvé un accord avec la Commission Européenne pour respecter un code de conduite. Toutefois, cette solution ne semble pas à ce jour convenir à plusieurs associations de défense des droits.

Les contenus illégaux bientôt bannis d'Internet ?

Depuis de longs mois maintenant, la Commission Européenne s'était fixée comme objectif d'éradiquer une majorité des propos haineux circulant sur la Toile.

Dans ce cadre, elle est parvenue à un accord avec YouTube, Microsoft, Twitter et Facebook pour l'établissement et le respect d'un code de conduite. Ainsi, les différents acteurs se sont engagés à bloquer les contenus gênants dans les 24 heures suivant leur signalement officiel.

En acceptant ce code de conduite pour bloquer les contenus illégaux, les acteurs du web montrent qu'ils ont bien conscience que leurs outils sont utilisés pour diffuser la violence et la haine mais aussi pour recruter des individus susceptibles de rejoindre leurs groupes.

Point positif, ce code de conduite ne vient pas entraver la liberté d'expression sur la Toile, celle-ci étant très importante en particulier pour les géants du web qui l'ont toujours prônée.

Un code de conduite pas suffisant selon les associations de défense des droits

Si la Commission Européenne s'est d'ores et déjà réjouie de l'accord trouvé avec les grandes entreprises du web, celui-ci ne fait assurément pas que des heureux.

En effet, Access Now et European Digital Rights (EDRi), deux associations de défense des droits, ont vivement critiqué cet accord estimant qu'il se contente de rappeler des règles déjà existantes à savoir celles qui consistent à supprimer des contenus illégaux.

Selon ces associations, il aurait donc fallu que le texte aille beaucoup plus loin et qu'il prévoit des poursuites contre ceux qui profèrent des propos haineux sur la Toile. En effet, Joe McNamee, Directeur Exécutif de l'EDRi, juge qu'« il est ironique que la Commission menace les Etats membres de les traduire en justice pour ne pas respecter les lois contre le racisme et la xénophobie alors qu'ils persuadent des entreprises comme Google et Facebook de glisser les infractions sous le tapis ».

Tout est dit…

Article original

Réagissez à cet article

Original de l'article mis en page : Les géants du web ensemble

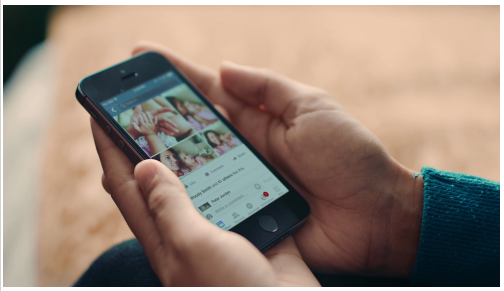
pour bloquer les contenus illégaux

Facebook vous traque sur le Web même si vous n’êtes pas membre

Facebook vous traque sur le Web même si vous n’êtes pas membre

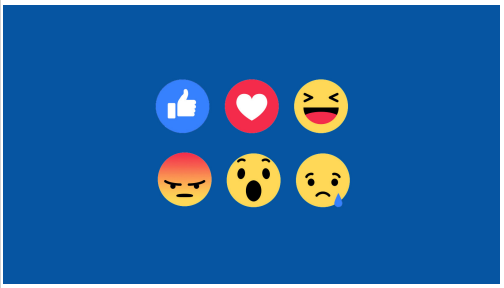
---

Facebook devient une régie publicitaire ouverte aux sites tiers, et affichera des publicités ciblées y compris pour les internautes qui ne sont pas inscrits sur le réseau social. Il utilisera ses scripts présents sur de nombreux sites pour suivre l'internaute dans ses déplacements sur le Web, et comprendre ce qui l'intéresse.

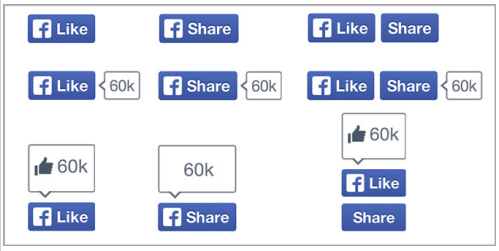


On connaît tous une ou deux personnes qui se refusent à utiliser Facebook et échappent encore et toujours aux griffes du réseau social. Mais l'empire de Mark Zuckerberg ne cesse de s'étendre et touchera bientôt même ces irréductibles qui n'ont jamais ouvert de compte sur la plateforme.

L'entreprise a annoncé qu'elle allait diffuser des annonces à tous les visiteurs de sites utilisant sa régie publicitaire Facebook Audience Network, concurrente de Google Adsense. Autrement dit, même les personnes qui ne sont pas inscrites sur Facebook et celles qui n'y sont pas connectées seront ciblées par des publicités qui, jusqu'ici, n'étaient visibles que par les personnes connectées au réseau social.
Ce n'est un secret pour personne, la force de Facebook réside dans sa capacité à récolter des données sur ses utilisateurs. Grâce à cela, il peut facilement montrer des publicités ciblées et adaptées sur mesure en fonction des préférences identifiées. Une aubaine pour les annonceurs qui ne perdent ainsi pas de temps et d'effort à diffuser tous azimuthes leurs contenus.



TRAQUER LES HABITUDES DE TOUS LES INTERNAUTES
Mais comment Facebook peut-il en faire de même avec les personnes qui ne se trouvent pas dans son réseau ? Il va utiliser plusieurs outils à sa disposition pour traquer efficacement un maximum d'internautes, comme le fait Google. Facebook va ainsi se servir de cookies, de ses propres boutons et plugins de partage affichés sur les sites, ainsi que d'autres informations collectées sur les sites tiers.
« Nos boutons et nos plugins envoient des informations de base sur les sessions de navigation des utilisateurs. Pour les non-membres de Facebook, auparavant nous ne les utilisions pas. Maintenant nous allons les utiliser pour mieux comprendre comment cibler ces personnes », assume très clairement Andrew Bosworth, vice-président de Facebook en charge des publicités et de la plateforme commerciale.



Ce dispositif permettra à Facebook de repérer les habitudes des internautes en insérant des bouts de codes dans les cookies et dans les boutons ou autres contenus « embeddés », qui permettront d'identifier l'internaute, soit directement en tant que membre de Facebook, soit par un numéro unique qui lui sera attribué. Si vous visitez régulièrement un site de cuisine, Facebook affichera des publicités pour une cocotte-minute ou une friteuse sur les autres sites que vous fréquentez, en rémunérant le site qui les affiche.

QUELLE LÉGALITÉ EN EUROPE ?
Ce changement de politique de Facebook va certainement mécontenter une partie de la communauté des internautes, y compris chez les membres qui pourront continuer à être suivis même lorsqu'ils sont déconnectés du réseau social. Elle pourrait surtout déclencher les foudres des autorités si le système est déployé en Europe.
Lorsque la justice belge avait condamné Facebook à ne plus tracer les Belges non-membres de Facebook, le réseau social s'était fait fort de crier à l'injustice, en prétendant que son cookie (le DATR) avait pour seul intérêt de lutter contre le spam. « Nous utilisons le cookie datr depuis plus de 5 ans pour sécuriser Facebook pour 1,5 milliard de personnes à travers le monde », s'était agacé le réseau social. Or six mois plus tard, Facebook prouve que les autorités avaient raison de s'inquiéter.
En France aussi, la Cnil a demandé à Facebook de ne plus tracer les internautes qui ne sont pas inscrits et connectés sur le réseau social. Avec d'autres homologues, elle avait estimé que Facebook devait « se conformer à ce jugement (belge) sur tout le territoire de l'Union européenne ».
Selon la législation européenne, il est illégal de réaliser un traitement de données personnelles à des fins commerciales, sans le consentement explicite de la personne. Or si ce consentement peut être donné à l'inscription par Facebook, il ne peut certainement pas l'être par les non-membres… [Lire la suite]

Article de Omar Belkaab

Réagissez à cet article

Source : *Facebook vous traquera sur le Web même si vous n'êtes pas membre – Business – Numerama*

Avec l'intelligence artificielle, Facebook en sait autant sur vous que votre conjoint

	Avec l'intelligence artificielle, Facebook en sait autant sur vous que votre conjoint. – Entreprises Numériques

---

Impossible d'échapper aux mécanismes de recommandations sur Internet. Tous les sites internet, marchands ou réseaux sociaux, utilisent désormais ces fameuses recommandations censées influencer nos comportements d'achats. Basées sur de l'intelligence artificielle de plus en plus puissante, les recommandations se font plus pertinentes. Dans l'avenir elles pourront tirer profit d'une connaissance précise de notre personnalité comme le montre une étude réalisée à partir de l'analyse des « likes » de Facebook.

Toute action sur Internet se transforme en données. On s'inquiète à juste titre de l'usage qui est fait de nos données personnelles (voir mon billet sur Safe Harbor). L'annonce par Facebook de « Search FYI » devrait encore attirer notre attention sur la protection de notre vie privée. Avec Search FYI, Facebook peut rechercher des informations dans tous les messages publics publiés par ses membres. Avec le développement de l'intelligence artificielle et l'utilisation du machine learning la valeur des données monte en flèche. Le mot « donnée » est souvent sous-estimé. On comprend bien qu'une photo et un texte postés sur un réseau social sont des données mais on oublie que le simple fait de cliquer sur un « like » devient une donnée aussi importante voire plus. Toute action sur internet laisse une trace numérique qui pourra être exploitée. C'est la base même du marketing digitale qui utilise ces traces numériques laissées sur le parcourt client pour mieux connaitre le consommateur et augmenter l'expérience utilisateur. C'est du donnant donnant : mieux nous sommes connus, mieux nous sommes servis. C'est l'évolution naturelle liée à la transformation numérique.
En analysant les « Likes », Facebook en sait plus sur notre personnalité que nos proches. La personnalité est un concept complexe qui semble difficilement mesurable. Cela touche à des sentiments, des émotions, des valeurs qui nous façonnent et qui nous rendent uniques. On pourrait donc imaginer, voire espérer, que les ordinateurs puissent se montrer impuissants à « quantifier » ce qui nous définit en tant qu'être humain. Pourtant une étude menée par des chercheurs des universités de Cambridge et de Stanford, publiée en janvier 2015, a montré que l'Intelligence Artificielle a le potentiel de mieux nous connaitre que nos proches. Cette étude visait à comparer la précision d'un jugement sur la personnalité réalisé par un ordinateur et des êtres humains. Les chercheurs ont demandé à 86.200 volontaires de leur donner accès à leurs « Likes » sur Facebook et de répondre à un questionnaire de 100 questions sur leur personnalité. Ces données ont été modélisées et le résultat est assez étonnant. On apprend que :
Avec l'analyse de 10 likes, Facebook en sait plus sur nous que nos collèges
Avec 70 likes Facebook en sait plus que nos amis
Avec 150 likes Facebook en sait plus que notre famille
Avec 300 likes Facebook en sait plus que notre conjoint
Quand on sait qu'en moyenne un utilisateur Facebook a 227 Likes, on se dit que nous n'avons plus grand choses à cacher.
Partager des émotions comme on partage des photos ou des vidéos. C'est la prochaine étape qu'imagine Mark Zuckerberg dans le futur. Durant une session de questions réponses sur son profile Facebook, le patron de Facebook a expliqué qu'il pensait que nous aurions à l'avenir la possibilité de partager nos expériences émotionnelles rien que par le seul fait d'y penser. La télépathie appliquée aux réseaux sociaux ? En matière d'Intelligence artificielle il devient difficile de faire la différence entre science-fiction et prévision. Quoiqu'il en soit Gartner a rappelé que c'étaient les algorithmes qui donnaient leur valeur aux données. Le progrès de ces algorithmes et leur complexité justifient qu'on s'intéresse à la protection de notre vie privée. Ils deviennent incontournables dans notre vie moderne, il faut en être conscient… [Lire la suite]

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.

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

Contactez-nous

Réagissez à cet article

Source : *Avec l'intelligence artificielle, Facebook en sait autant sur vous que votre conjoint. – Entreprises Numériques*

Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google

Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google

---

Le lanceur d'alerte à l'origine du scandale de la surveillance de la NSA et des spécialistes en sécurité informatique mettent en cause la politique de chiffrement mise en place par Google pour sa nouvelle messagerie.

Haro sur Allo. La nouvelle application de messagerie instantanée de Google était l'une des principales annonces de la conférence Google I/O, mercredi 18 mai, au quartier général de l'entreprise à Mountain View. Fondée sur l'intelligence artificielle, elle est capable de comprendre le langage humain et affine son algorithme au fil des conversations afin de proposer des suggestions de plus en plus pertinentes. Disponible cet été sur Android et iOS, elle est déjà au coeur d'une controverse d'experts.
Allo possède des paramètres de sécurité renforcés. Un mode « incognito » permet de chiffrer de bout en bout les messages afin de les rendre illisibles pour une personne extérieure à la conversation. Seuls les participants à la discussion sont en mesure de les déchiffrer. Google lui-même ne peut pas y accéder et répondre à d'éventuelles requêtes judiciaires des autorités.
Cette option est basée sur le protocole open source Signal, développé par Open Whispers Systems. C'est le même protocole de chiffrement que WhatsApp, dont les discussions sont cryptées de bout en bout depuis le mois d'avril. Mais à l'inverse de WhatsApp et d'autres messageries sécurisées actuelles (Viber, Signal, iMessage) le chiffrement des conversations n'est pas activé par défaut sur Allo. C'est aux utilisateurs d'effectuer la démarche.

Les experts en sécurité déconseillent Allo

Des experts en cybersécurité s'interrogent déjà sur la pertinence d'une telle fonction, arguant que de nombreux utilisateurs ne feront pas la démarche de l'activer. « La décision de Google de désactiver par défaut le chiffrement de bout en bout dans la nouvelle application de discussion instantanée Allo est dangereuse et la rend risquée. Évitez-la pour l'instant », a conseillé Edward Snowden sur Twitter.
Le lanceur d'alerte à l'origine du scandale des programmes de surveillance de la NSA en 2013 n'est pas le seul à critiquer le choix de Google. Nate Cardozo, représentant de l'EFF, une association américaine de défense des libertés numériques, a estimé pour sa part que « présenter la nouvelle application de Google comme étant sécurisée n'est pas juste. L'absence de sécurité par défaut est l'absence de sécurité tout court ».
« Rendre le chiffrement optionnel est une décision prise par les équipes commerciales et juridiques. Elle permet à Google d'exploiter les conversations et de ne pas agacer les autorités », a encore indiqué Christopher Soghoian, membre de l'Association américaine pour les liberté civiles.

L'intelligence artificielle, priorité de Google

Après avoir pris fait et cause pour Apple dans le bras de fer qui l'a opposé au FBI sur le déblocage de l'iPhone chiffré d'un des terroristes de San Bernardino, Google n'est donc pas allé aussi loin que WhatsApp en généralisant le chiffrement des discussions. Un ingénieur en sécurité de Google a expliqué sur son blog comment la société avait dû arbitrer entre la sécurité des utilisateurs et les services d'intelligence artificielle d'Allo.
Pour profiter pleinement des capacités de Google Assistant implémentées dans Allo, les algorithmes doivent être en mesure d'analyser les conversations, ce qui n'est possible qu'en clair. « Dans le mode normal, une intelligence artificielle lit vos messages et utilise l'apprentissage automatique pour les analyser, comprendre ce que vous voulez faire et vous donner des suggestions opportunes et utiles », explique Thaï Duong.
Ce parti pris pourrait évoluer d'ici la sortie de l'application cet été. Le site américain TechCrunch a publié des paragraphes que l'ingénieur avait publié dans son article avant de les supprimer. Il affirme qu'il est en train de « plaider en faveur d'un réglage avec lequel les usagers peuvent choisir de discuter avec des messages en clair », pour interagir avec l'intelligence artificielle en l'invoquant spécifiquement, sans renoncer à la vie privée. En somme, proposer « le meilleur des deux mondes »… [Lire la suite]

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.

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

Contactez-nous

Réagissez à cet article

Source : *Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google*

Entreprises, surveillez l'usage des réseaux sociaux !

Entreprises, surveillez l'usage des réseaux sociaux !

Selon Osterman Research, près de une entreprise sur cinq a été victime de malwares diffusés par le biais de réseaux sociaux.

Les réseaux sociaux sont des outils de communication clés pour les entreprises, mais ils constituent aussi un vecteur d'attaques informatiques encore trop souvent négligé par les organisations, observe le cabinet américain Osterman Research dans un livre blanc (Best Practices for Social Media Archiving and Security). Sponsorisée par Actiance, Gwava et Smarsh, l'enquête a été réalisée auprès d'un panel de professionnels IT et décideurs d'entreprises de taille moyenne et de grands groupes.
73 % des entreprises concernées par cette enquête utilisent Facebook dans le cadre professionnel, 64 % LinkedIn et 56 % Twitter. Plusieurs plateformes sont utilisées régulièrement. Du côté des réseaux sociaux d'entreprise (RSE), Microsoft Sharepoint est l'outil le plus largement cité (par 82 % des répondants). Il devance Jabber et WebEx de Cisco ou encore Yammer de Microsoft.

Une porte d'entrée pour les malwares
54 % des organisations ont adopté une politique relative à l'utilisation par leurs collaborateurs des réseaux sociaux tout public (ce taux passe à 51 % pour les RSE). Mais elles ne sont plus que 48 % à le faire lorsqu'il est question de l'usage professionnel des plateformes tout public. Si une majorité veille ou surveille cet usage, 27 % ne le font pas. Et ce malgré les cybermenaces et les risques juridiques auxquels les entreprises sont confrontées.
Dans ce contexte, 18 % ont constaté que leur compte « social » a été piraté ou ont été victime d'une attaque par malware, soit près d'un utilisateur de réseau social sur cinq en entreprise. Mais pour 80 % des répondants, c'est bien l'email qui constitue la première source d'infiltration de logiciels malveillants dans les systèmes et réseaux internes des organisations
[Lien vers l'article original partagé]

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.

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

Contactez-nous

Réagissez à cet article

Source : *Sécurité : entreprises, surveillez l'usage des réseaux sociaux !*

Plus de 100 millions de mots de passe LinkedIn dans la nature… depuis 2012 !

Plus de 100 millions de mots de passe LinkedIn dans la nature… depuis 2012 !

Une base de données, contenant 117 millions de combinaisons d'identifiants et de mots de passe, est vendue 2000 euros par des pirates. Le réseau social professionnel enquête.

Le piratage massif dont a été victime LinkedIn en 2012 revient hanter le réseau social professionnel. Une base de données contenant plus de 100 millions d'identifiants et de mots de passe est actuellement proposée à la vente sur une place de marché du dark web, «The Real Deal», rapporte le siteMotherBoard. Le fichier est proposé à la vente pour 5 bitcoins, soit un peu plus de 2000 euros. Il concerne 167 millions de comptes, dont 117 millions sont associés à un mot de passe.

Le site LeakedSource, qui a eu accès au fichier, assure avoir réussi à déchiffrer en trois jours «90% des mots de passe». Ils étaient en théorie protégés par un procédé de hachage cryptographique, SHA-1, mais sans salage, une technique compliquant leur lecture en clair. Deux personnes, présentes dans le fichier, ont confirmé à un chercheur en cybersécurité que le mot de passe associé à leur identifiant était authentique.

LinkedIn avait reconnu en 2012 le vol des données de connexion, mais sans jamais préciser le nombre d'utilisateurs concernés. Un fichier, concernant 6,5 millions de comptes, avait à l'époque été mis en ligne. «À l'époque, notre réponse a été d'imposer un changement de mot de passe à tous les utilisateurs que nous pensions touchés. De plus, nous avons conseillé à tous les membres de LinkedIn de changer leurs mots de passe», commente aujourd'hui le réseau social professionnel sur son blog.

123456, linkedin, password, 123456789 et 12345678

En réalité, un porte-parole de LinkedIn avoue «ne pas savoir combien de mots de passe ont alors été récupérés». «Nous avons appris hier qu'un jeu de données supplémentaire qui porterait supposément sur plus de 100 millions de comptes et proviendrait du même vol de 2012, aurait été mis en ligne. Nous prenons des mesures immédiates pour annuler ces mots de passe et allons contacter nos membres. Nous n'avons pas d'éléments qui nous permettent d'affirmer que ce serait le résultat d'une nouvelle faille de sécurité», ajoute LinkedIn sur son blog.

Selon LeakedSource, la base de données aurait été détenue jusqu'alors par un groupe de pirates russes. Ces informations de connexion, même si elles remontent à 2012, ont encore une grande valeur. Elles peuvent être utilisées tout à la fois pour pénétrer dans d'autres comptes plus critiques (sites d'e-commerce, banque en ligne…) ou organiser des campagnes de phishing, une technique utilisée pour obtenir les renseignements personnels d'internautes. Nombre d'utilisateurs utilisent la même combinaison d'adresse email et de mot de passe sur tous les sites, et en changent peu souvent, ce qui démultiplie les effets de tels piratages.Preuve de cette imprudence générale, les cinq mots de passe les plus utilisés dans le fichier mis en vente étaient 123456, linkedin, password, 123456789 et 12345678… [Lire la suite]

Réagissez à cet article

Source : *Plus de 100 millions de mots de passe LinkedIn dans la nature*

Et si la reconnaissance faciale de Facebook était excessive ?

Et si la reconnaissance faciale de Facebook était excessive ?

Depuis 2010, Facebook propose à ses utilisateurs un système de reconnaissance faciale qui permet de gagner du temps dans le « taguage » des personnes qui sont sur les photos. Sous couvert d'une nouvelle fonctionnalité, c'est un véritable dispositif biométrique qui a été mis en œuvre car il permet d'identification d'un individu à partir d'une simple photographie de son visage.

En Californie, trois utilisateurs ont reproché au réseau social n°1 d'avoir « secrètement et sans leur consentement » collecté des « données biométriques dérivées de leur visage ». Ces plaintes ont été jugées recevables par le juge James Donato qui « accepte comme vraies les allégations des plaignants » et juge « plausible » leur demande.

Au sein de l'Union européenne, le danger a rapidement été perçu s'agissant du système de reconnaissance faciale de Facebook qui l'a suspendu en 2012. Mais aux Etats-Unis, bien moins vigilants, cette fonctionnalité a perduré et il apparait bienvenu que la Justice y réagisse enfin. Facebook a constitué des profils qui répertorient les caractéristiques du visage de ses utilisateurs, leur cercle d'amis, leurs goûts, leurs sorties, etc. Avec plus de 3 milliards d'internautes dans le monde, cela revient à ce qu'environ 28% de la population ait un double virtuel rien que sur Facebook.

Facebook is watching you : Reconnaissance faciale, intelligence artificielle et atteinte aux libertés

Eu égard à leur grand potentiel discriminatoire, les données biométriques sont strictement encadrées par la loi du 6 janvier 1978 puisque d'après son article 25, une autorisation préalable de la Commission nationale de l'informatique et des libertés est indispensable pour mettre en œuvre des « traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes ». Cela regroupe l'ensemble des techniques informatiques qui permettent d'identifier un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.

Les conditions générales d'utilisation de Facebook ne sont pas donc pas conformes à la législation française sur les données personnelles, notamment s'agissant de la condition de consentement préalable, spécifique et informé au traitement des multiples données à caractère personnel collectées. Mais le géant de l'internet ne répond qu'à l'autorégulation. Par opposition à la règlementation étatique, la régulation n'entend prendre en compte que la norme sociale, c'est-à-dire l'état des comportements à un moment donné. Si la norme sociale évolue, alors les pratiques de Facebook s'adapteront.

Vers une remise en cause mondialisée des abus de Facebook ?

L'affaire pendante devant les Tribunaux met en lumière le manque de réactivité des américains face aux agissements de Facebook. C'est seulement au bout de 5 années que la Justice s'empare de la question des données biométriques à l'initiative de simples utilisateurs, alors même qu'une action de groupe à l'américaine d'envergure aurait pu être engagée pour mettre sur le devant de la scène les abus de Facebook.

Néanmoins, « mieux vaut tard que jamais » et l'avenir d'une décision répressive ouvre la porte vers de nouveaux horizons pour l'ensemble des utilisateurs. En effet, Facebook prend comme modèle pour toutes ses conditions générales d'utilisation à travers le monde la version américaine de « licencing ». Plus Facebook se verra obligé dans son pays natal à évoluer pour respecter les libertés individuelles des personnes inscrites, plus on s'éloignera du système tentaculaire imaginé par Mark Zuckerberg qui n'est pas sans rappeler celui imaginé par Georges Orwell dans son roman 1984.

Par Antoine CHERON, avocat associé, est docteur en droit de la propriété intellectuelle, avocat au barreau de PARIS et au barreau de BRUXELLES et chargé d'enseignement en Master de droit à l'Université de Assas (Paris II). Il est le fondateur du cabinet d'avocats ACBM… [Lire la suite]

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.

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

Contactez-nous

Réagissez à cet article

Source : *Facebook is watching you : système biométrique efficace – Data Security BreachData Security Breach*

Top 10 des arnaques sur Facebook en 2014

Top 10 des arnaques sur Facebook en 2014

Une étude des analystes antivirus Bitdefender révèle que Taylor Swift n'est plus aussi populaire que l'année dernière, lorsqu'une fausse vidéo à son sujet avait permis de répandre massivement un malware sur le réseau social. Chaque année, des millions d'utilisateurs tombent dans les pièges des arnaques diffusées sur Facebook. Voici le classement des 10 arnaques les plus répandues dans le monde, depuis le début de l'année 2014 !

1. **Qui a visité mon profil**– 30.20% (anglais – international)
2. **Changez la couleur de votre Facebook** – 7.38% (anglais – international)
3. **La sextape de Rihanna avec « son » petit-ami**– 4.76% (anglais – international)
4. **Consultez mon nouveau statut pour recevoir gratuitement un T-shirt officiel Facebook** – 4.21% (anglais – international)
5. **Dites au revoir au Facebook bleu**– 2.76% (français)
6. **Produits défilmés. Distribution gratuite**– 2.41% (anglais – international)
7. **Vérifiez si un ami vous a supprimé de sa liste** – 2.27% (anglais – international)
8. **Cliquez ici pour voir le top 10 des profils qui vous harcèlent le plus ! Vous serez étonné d'apprendre que votre ex visite toujours votre profil !** – 1.74% (anglais – international)
9. **Découvre comment voir qui visite ton profil, tu n'es pas au bout de tes surprises !** – 1.55% (espagnol)
10. **Je viens de modifier le thème de mon Facebook. C'est incroyable**– 1.50% (anglais – international)

Autres : 41.22%

Alors que Taylor Swift quitte le Top 10, **Rihanna reste la star la plus utilisée en tant qu'« appât »** par les scammers pour répandre un malware via Facebook.
L'arnaque des billets "gratuits" pour Disneyland sort aussi du classement alors qu'en juillet dernier, elle surclassait l'arnaque « Je peux vérifier qui regarde mon profil » qui avait fait des dizaines de milliers de victimes. Le scam « **Qui a visité mon profil » conserve quant à lui sa 1ère place**, représentant presque un tiers de la part totale des arnaques sur Facebook (30.20%).
Les arnaques du type « changez la couleur de votre Facebook » se sont internationalisées et représentent dorénavant **7,38 % de la part totale des scams sur Facebook** (vs 4.16% en 2013).

Les mêmes arnaques Facebook fonctionnent toujours

« Pourquoi les utilisateurs veulent-ils toujours savoir qui a jeté un coup d'œil à leur profil, malgré tous les avertissements de sécurité à ce sujet ? » déclare Catalin Cosoi, Responsable de la Stratégie de sécurité chez Bitdefender. *« Ils pensent certainement qu'il s'agit de vraies applications… C'est ce que l'on appelle de l'ingénierie sociale, et elle atteint alors son plus haut niveau – un jeu psychologique entre le cybercriminel et sa victime. Les appâts ont changé avec le temps – harceleurs, voyeurs, admirateurs, petites amies trop attachées et ex qui vous hantent, mais la raison pour laquelle ces arnaques fonctionnent est simple : la nature humaine. »*
Une offre de **T-shirts Facebook gratuits** fait son entrée dans le Top 10 (4.21 %). Les fans intéressés par des vêtements à l'effigie de la marque américaine se retrouvent à remplir de **fausses études ou à installer des add-ons malveillants** qui exploitent leurs données personnelles.
L'autre nouveauté de ce classement concerne des arnaques qui piègent les utilisateurs avec des **cadeaux publicitaires défilmés** (2,41 %).
Au cours de ces deux dernières années, les **arnaques sur Facebook se sont multipliées** en même temps que la plate-forme de réseau social s'est développée. L'étude Bitdefender montre aussi une augmentation du nombre d'arnaques via des **vidéos virales qui utilisent de façon abusive les "*like*"** Facebook et les options de partage. L'année passée, les sites frauduleux utilisant le **likejacking** (détournement de « *J'aime*«), **clickjacking** (détournement de liens) et **YouTube** ont proliféré en anglais mais aussi en allemand, chinois et en italien.
Pour éviter d'être détectés plus facilement, les scammers peuvent utiliser des caractères spéciaux et numéros dans la description de leur fausse application. Une **variante populaire du scam « Top profil visiteurs »** attire de nouvelles victimes avec ce message : *"Check 0ut n0w wh0 viewed ur profile"*.
Cette étude se base sur les données issues de l'outil Safego de Bitdefender, l'application Facebook gratuite qui scanne les timelines et alerte les utilisateurs en cas de posts malveillants et frauduleux. Pour plus d'informations sur la protection de vos comptes utilisateurs de médias sociaux, vous pouvez consulter le guide de sécurité de Bitdefender à ce sujet… [Lire la suite]

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.

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

Contactez-nous

Réagissez à cet article

Source : *Fausses sextapes et arnaques diverses : le top 10 des scams en 2014 sur Facebook*

Paypal ne protégera plus les transactions crowdfunding

Paypal ne protégera plus les transactions crowdfunding

Trop d'arnaques au financement participatif ? Trop de remboursements pour des produits jamais livrés ? Paypal ne protégera plus les transactions crowdfunding à partir de la fin juin 2016.

Paypal semble ne plus apprécier les transactions bancaires entre ses utilisateurs et les projets lancés sur les portails de crowdfunding. Trop d'arnaques au Crowdfunding ? Á partir du 26 juin 2016, le géant de la finance, ne protégera plus les transactions effectuées sur les sites de financement participatif.
Trop d'arnaques au transactions crowdfunding ? Trop d'argent envolé sans le moindre produit/projet finalisé ? Bref, des problèmes se posent des deux côtés – vendeurs et acheteurs. Paypal ne veut tout simplement plus faire partie d'une équation qui le place au milieu des conflits. Par conséquent, vous pourrez toujours payer via Paypal, mais la structure financière n'assurera plus cette transaction. Elle sera à vos risques et périls.

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.

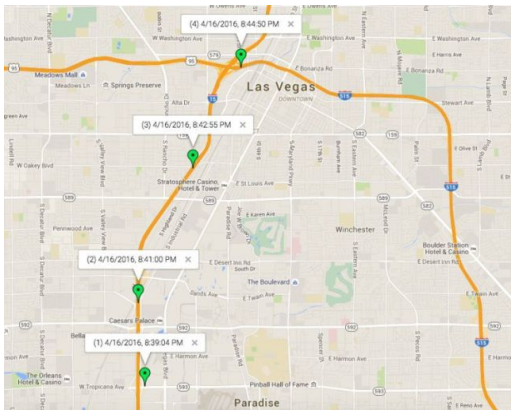
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *ZATAZ Paypal ne protégera plus les transactions crowdfunding – ZATAZ*

Waze : les hackeurs peuvent vous suivre à la trace

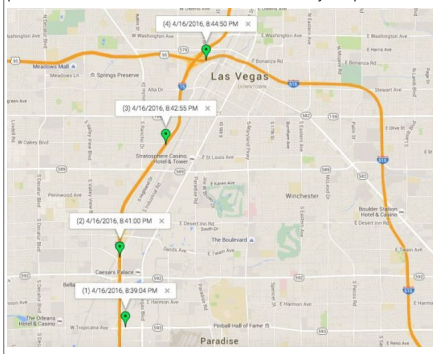


Waze : les hackeurs peuvent vous suivre à la trace

Des experts en sécurité informatique ont découvert une faille permettant d'espionner en temps réel les trajets des utilisateurs de l'application de navigation communautaire Waze. Selon eux, presque toutes les applications d'aide à la conduite seraient concernées. Explications.

C'est l'une des applications d'aide à la conduite les plus populaires en France. Aujourd'hui, près de 5 millions d'automobilistes utilisent presque quotidiennement le service de navigation communautaire Waze. Il a y a quelque mois, des chercheurs de l'Université de Californie à Santa-Barbara (Etats-Unis) ont découvert une faille, partiellement corrigée seulement, qui permet à des hackeurs d'espionner en temps réel les déplacements de n'importe quel utilisateur.
L'équipe d'experts en sécurité informatique a suivi durant trois jours les trajets d'une journaliste du site américain Fusion. Afin de vous livrer les informations de trafic, Waze utilise une connexion sécurisée pour communiquer avec votre smartphone. Or c'est justement là que se trouve la faille. Les chercheurs sont parvenus, en effet, à se placer entre les serveurs de l'application et l'utilisateur. De ce fait, ils ont pu intercepter toutes ses données de navigation, ainsi que ses trajets en bus ou en taxi.

Voiture fantôme, véhicule espion, embouteillage virtuel
Une fois infiltrés dans les serveurs de l'application, ils ont pu étudier en détail le fonctionnement des algorithmes de Waze. Au-delà des problèmes de confidentialité, les chercheurs se sont aperçus qu'ils pouvaient également créer des véhicules « fantômes ». Dans le but, par exemple, de créer de faux embouteillages ou d'épier tous les utilisateurs se trouvant à proximité de ce conducteur virtuel. En envoyant plusieurs véhicules fantômes, ils affirment avoir été en mesure de quadriller un quartier entier.



D'après ces experts en sécurité en informatique, il serait même possible de surveiller l'intégralité de la population américaine, simplement "en utilisant quelques serveurs de plus". Imaginez : tous vos trajets pourraient être enregistrés et mis à disposition du plus offrant. L'équipe de recherche a informé Waze de sa découverte, il y a plusieurs mois, et l'application, rachetée par Google en 2013, avait procédé à une mise à jour. Mais elle ne corrige que partiellement la faille.
« Toutes ont quasiment toutes ce type de failles »
Depuis janvier dernier, les données de géolocalisation ne sont plus partagées avec les conducteurs situés à proximité lorsque l'application est ouverte en tâche de fond. En revanche, il est toujours possible de vous espionner lorsqu'elle est en marche. Mais la faille est toujours présente quand on l'utilise en premier plan.

Comment faire ? ⇒ Seule solution pour le moment : utiliser le mode invisible… qui se désactive automatiquement à chaque redémarrage de l'application.

Waze semble être en effet conscient de ses lacunes. Dernièrement, l'application a mis en place une fonction censée permettre à son utilisateur de masquer son emplacement réel. Cependant, comme on le démontre l'enquête de Fusion, ce nouveau système n'est pas vraiment efficace. Et surtout, elle n'est pas à la seule application concernée, si l'on en croit Ben Zhao : « Nous avons étudié de nombreuses applications. Presque toutes ont ce type de failles. Nous ne savons pas comment stopper cela », s'inquiète Zhao. Pas de quoi rassurer les automobilistes… [Lire la suite]

Réagissez à cet article

Source : *Waze : les hackeurs peuvent vous suivre à la trace – metronews*