

Pokémon Go peut-il vraiment prendre le contrôle de votre compte Gmail ?



Pokémon
Go peut-
il
vraiment
prendre
le
contrôle
de votre
compte
Gmail ?

Malgré son succès indéniable, il semblerait que l'application Pokémon Go rencontre des premiers couacs, notamment en matière de protection de la vie privée. Selon certaines informations, depuis démenties, elle pourrait accéder et composer des emails sur le compte Gmail des utilisateurs.

Après avoir soulevé certains problèmes récemment avec le cas des voleurs armés aux États-Unis qui utilisaient le jeu pour cibler leurs victimes ou celui d'une jeune adolescente qui aurait retrouvé un cadavre pendant sa « chasse » aux Pokémon. La polémique n'en finit plus autour de Pokémon Go. C'est aujourd'hui un problème d'éthique et de sécurité qui est désormais pointé du doigt.

Pokémon Go : comment le jeu a rendu fou le monde entier

En effet lorsque vous installez et que vous jouez à Pokémon Go pour la première fois, le jeu sur smartphone développé par la firme Niantic, demande deux types de connexion. La première consiste à créer un compte via l'application tandis que la deuxième exige de se connecter directement depuis son compte Google. C'est la deuxième connexion qui soulève plusieurs problèmes.

Sur son blog, l'analyste en sécurité Adam Reeve expliquait ainsi ce week-end que cette identification par Google pouvait poser plusieurs problèmes puisque l'application accédait à plusieurs paramètres de votre compte Google : « Pokémon Go et Niantic peuvent désormais lire tous vos emails, envoyer des emails de votre part, accéder à vos documents Google Drive, rechercher dans votre historique de recherche et de navigation, accéder à toutes les photos privées hébergées sur Google Photos et bien davantage ». Des accès qui ne sont, bien évidemment, pas nécessaires pour profiter de l'expérience de jeu de l'application développée par Niantic.

Des informations démenties par Google et Niantic

Cependant, interrogé par le site Gizmodo, Adam Reeve a finalement fait marche arrière sur ses affirmations, expliquant ne pas être « certain à cent pour cent » que son billet de blog est exact. Il a par ailleurs expliqué au site Internet qu'il n'avait jamais développé lui-même d'application utilisant l'identification Google et n'a pas expérimenté ce qu'il indiquait sur son blog.

Du côté de Google également, l'information a été démentie auprès de Dan Guido, expert en sécurité informatique. La firme de Mountain View explique que les autorisations de Pokémon Go ne concernent que la partie « Mon Compte » de Google et n'autorise pas d'accès spécifique à différents services. Enfin, le studio Niantic, qui développe l'application avec The Pokémon Company, a publié ce mardi un communiqué de presse afin de rassurer les utilisateurs : « Pokémon Go n'accède qu'aux informations basiques des profils Google (votre identification et votre adresse email). Aucune autre information de votre compte Google n'est ou ne sera collectée. [...] Google réduira prochainement les autorisations de Pokémon Go uniquement aux données de profil dont Pokémon Go a besoin, les utilisateurs n'auront pas besoin d'effectuer le moindre changement ».

Article original de GEOFFROY HUSSON



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

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



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Pokémon Go peut-elle vraiment prendre contrôle de votre compte Gmail ?

Les géants d'internet contrôlent de plus en plus l'information



Les géants
d'internet
contrôlent de
plus en plus
l'information

Entre les médias et les lecteurs, l'information passe aujourd'hui le plus souvent par les algorithmes des géants d'internet, qui contrôlent de fait ce flux et une bonne partie des revenus qu'il génère. Au point de susciter des inquiétudes.

« Ces 18 derniers mois, (ces géants d'internet) qui avaient jusqu'ici une relation distante avec le journalisme sont devenus des acteurs dominants de l'écosystème de l'information », résume le Tow Center for Digital Journalism de l'Université américaine de Columbia, dans une étude publiée en juin 2016. Beaucoup proposent aux éditeurs de presse de publier directement leur contenu sur leurs plateformes, à l'instar des canaux Instant Articles de Facebook ou Discover de Snapchat, et sont « désormais directement impliqués dans tous les aspects du journalisme », fait valoir l'étude. La plupart des médias nouent des partenariats avec ces nouveaux acteurs de l'information pour maintenir ou développer leur exposition sur les moteurs de recherche et les réseaux sociaux, mais les perspectives financières restent incertaines.

« Il y a des gens qui font de l'argent sur internet, mais pas les médias, qu'ils soient tous supports ou uniquement en ligne », affirme une autre étude, du centre indépendant Pew Research Center, publiée mi-juin. Elle souligne ainsi qu'en 2015, 65% des revenus publicitaires en ligne étaient concentrés par cinq places fortes du web, Google, Facebook, Microsoft, Yahoo et Twitter, une proportion en hausse par rapport à 2014 (61%). Tout comme le modèle économique, c'est aussi le contenu et sa hiérarchie qui leur échappent, soumis au filtre des algorithmes. « L'impact que ces sociétés technologiques ont sur le secteur du journalisme va bien au-delà de l'aspect financier, jusqu'à ses composantes les plus essentielles », considère l'institut Pew.

Désormais, les géants d'internet « supplantent les choix et les objectifs des sites d'information et leurs substituent (les leurs) », affirme l'étude. Si certains y voient l'occasion d'une démocratisation de l'information, d'autres s'inquiètent d'une altération de sa qualité. « Vous n'avez aucune idée de ce que les gens vont voir et il se peut tout à fait que (ce soit) quelque chose d'assez léger plutôt que des informations majeures », prévient Dan Kennedy, professeur de journalisme à l'Université Northeastern.

Le secret des algorithmes

Une étude réalisée par Nic Newman du Reuters Institute a fait état de « préoccupations liées à la personnalisation des informations et une sélection algorithmique qui pourraient passer à côté de nouvelles importantes et de points de vue différents », selon le blog de son auteur. Mais « les jeunes préfèrent les algorithmes aux éditeurs » qui organisent l'information, constate-t-il. Ce pouvoir croissant des incontournables d'internet a attiré l'attention début mai lorsque le site d'information Gizmodo a accusé, témoignages à l'appui, Facebook d'avoir manipulé son fil de tendances. Après enquête interne, le plus grand réseau social du monde a conclu qu'il n'y avait pas eu de démarche concertée ou de manipulation, mais s'est engagé à préserver la neutralité de sa plateforme.

« Nous sommes une entreprise technologique, pas un média », a expliqué récemment la directrice d'exploitation de Facebook, Sheryl Sandberg, lors d'une table ronde à Washington. « Nous n'essayons pas de recruter des journalistes ou de rédiger des nouvelles », a-t-elle martelé. Pour autant, l'intervention humaine reste nécessaire, selon elle, « parce que sans cela, tous les jours à midi, le déjeuner serait une tendance ». Même si la hiérarchisation des informations est largement automatisée sur ces plateformes, les programmes qui régissent ce processus sont bien rédigés par des humains qui opèrent, pour ce faire, des choix. Cela pose, dès lors, « des questions quant à la transparence » de l'ensemble, souligne Nicholas Diakopoulos, professeur de journalisme à l'université du Maryland. « Il pourrait être intéressant de savoir de quelles données se nourrit le logiciel ou quels sites il suit », estime l'universitaire, pour qui « il faut réfléchir à des normes de transparence ».

Une étude publiée l'an dernier a révélé que le trafic des principaux sites d'information en provenance de Facebook avait chuté de 32% après une modification des algorithmes du réseau social. « Il est vrai que Facebook peut faire décoller ou tuer un site d'information selon la façon dont il calibre son algorithme », reconnaît Nikki Usher, professeure de nouveaux médias à l'Université George Washington. « D'un autre côté, les médias n'ont jamais eu à rendre de compte sur les décisions qu'ils prenaient » en matière éditoriale, fait-elle valoir.

Article original de Joël Ignasse



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

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

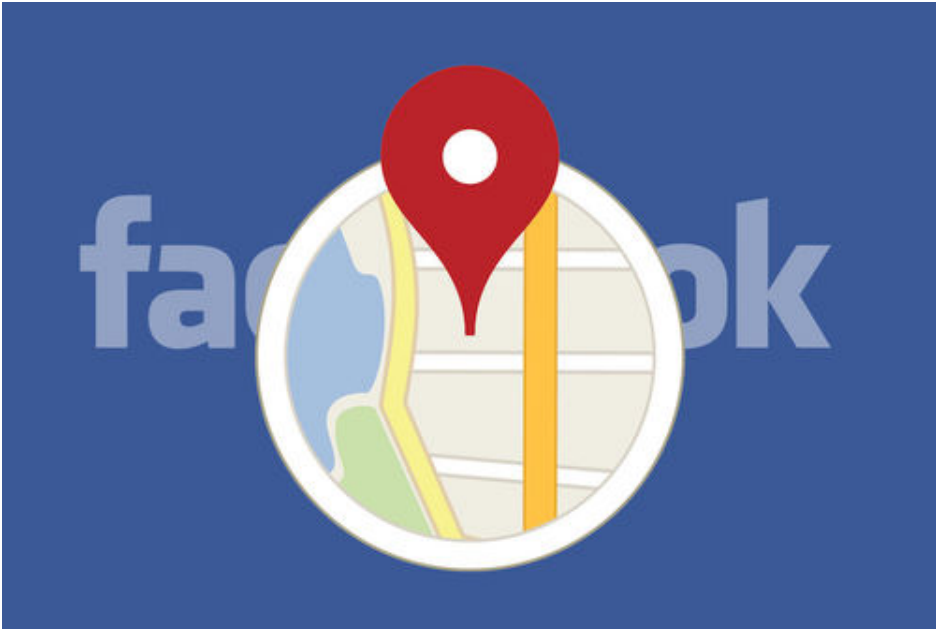


[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Les géants d'internet contrôlent de plus en plus l'information – Sciencesetavenir.fr

Facebook vous suit à la trace pour vous suggérer des amis

 A blue rectangular box containing the Facebook logo in a lighter blue font. Overlaid on the logo is a circular icon with a white border. Inside the circle is a stylized map with yellow roads and green areas. A red location pin with a white dot is placed on the map.	Facebook vous suit à la trace pour vous suggérer des amis
---	--

La géolocalisation de Facebook, utilisée notamment sur l'application mobile du réseau social, faisait déjà l'objet de nombreuses suspicions de la part des utilisateurs. Cette semaine, un porte-parole de Facebook a confirmé que la position géographique avait effectivement été utilisée par l'application pour suggérer de contacts que vous auriez pu croiser.

La fonction « Vous connaissez peut-être » de Facebook est souvent surprenante par sa précision, suggérant généralement des contacts pertinents. Si le site n'a jamais révélé vraiment les méthodes utilisées pour faire mouche aussi souvent, un de ses secrets vient en revanche d'être découvert : la géolocalisation permettrait de déterminer les personnes que vous fréquentez et qui disposent d'un compte. Concrètement, si deux personnes disposant d'un compte Facebook se trouvent au même endroit et ont activé la géolocalisation, le site proposera alors de les mettre en relation sur le réseau social. « La localisation elle-même ne suffit pas à déterminer que deux personnes peuvent être amies », indique un porte-parole de Facebook au journal anglais The Telegraph. Et c'est justement un des arguments avancés par les détracteurs de cette fonction, qui y voient une atteinte à la vie privée. Le site n'étant pas capable de déterminer si deux personnes se trouvant au même endroit sont amies, ou même si elles se connaissent réellement, l'usage d'une telle fonction peut sembler abusif sur certains aspects, et poser quelques problèmes concernant l'anonymat que certains voudraient conserver en public. Facebook a cependant indiqué que cette fonction n'était aujourd'hui plus active sur son application mobile, et que celle-ci avait simplement fait l'objet d'un test limité. Les plus inquiets peuvent néanmoins désactiver la géolocalisation pour l'application.

Article original de Nicolas AGUILA



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

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



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Facebook vous suit à la trace pour vous suggérer des amis

Russie : Edward Snowden dénonce une loi « Big Brother » et la « surveillance de masse » en Russie

Denis JACOPINI



vous informe

Edward Snowden
dénonce une loi
« Big Brother »
et la «
surveillance de
masse » en
Russie

Edward Snowden, l'ancien agent du renseignement américain réfugié en Russie, a dénoncé samedi 25 juin les lois antiterroristes adoptées par les députés russes. Ces dernières relèvent selon lui de « Big Brother » et de la « surveillance de masse », et a demandé qu'elles ne soient pas promulguées.



« La nouvelle loi russe Big Brother constitue une violation inapplicable et injustifiable des droits qui ne devrait jamais être promulguée », a écrit sur Twitter le lanceur d'alerte, qui a fui les Etats-Unis pour révéler l'ampleur de la surveillance menée par les services de renseignement américains.

« La surveillance de masse ne marche pas. Ce texte va coûter de l'argent et de la liberté à chaque Russe sans améliorer la sécurité », a-t-il insisté dans un second message.

Des lois extrêmement répressives

Adoptés vendredi lors de la dernière séance de la Douma (chambre basse) avant les législatives du 18 septembre, les projets de loi en question obligent en particulier les opérateurs de télécommunications et internet à stocker les messages, appels et données des utilisateurs pendant six mois pour les transmettre aux « agences gouvernementales appropriées » à leur demande.

Les réseaux sociaux se voient également obligés de stocker les données pendant six mois, selon l'un de ces textes qui doivent encore être approuvés par le Conseil de la Fédération (chambre haute) et promulgués par M. Poutine.

Ce délai de six mois « n'est pas seulement dangereux, il est inapplicable », a prévenu M. Snowden, qui avait été critiqué, par le passé, pour ne pas critiquer assez sévèrement le régime de Vladimir Poutine.

Ces lois ont été dénoncées par l'opposition russe comme une tentative de « surveillance totale » de la part des autorités, mais aussi par les entreprises du numérique qui ont critiqué un coût exorbitant.

Elles introduisent par ailleurs des peines de prison pour la non-dénonciation d'un délit, abaissent l'âge de la responsabilité pénale à 14 ans et introduisent des peines allant jusqu'à sept ans de détention pour la « justification publique du terrorisme », y compris sur internet.

Article original Le Monde



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

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



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Russie : Edward Snowden dénonce une loi « Big Brother » et la « surveillance de masse »

Enquête sur l'algo le plus flippant de Facebook



Enquête
sur
l'algo
le plus
flippant
de
Facebook

La section « Vous connaissez peut-être » (« People you may know ») de Facebook est une source inépuisable de spéculations. Cette fonction, en apparence sympathique puisqu'elle nous propose d'ajouter de nouveaux amis, semble détenir des informations très personnelles sur chacun d'entre nous.

- Beaucoup ont aussi vu apparaître des gens rencontrés sur des applis de rencontre comme Tinder ou Grindr. Plutôt embarrassant, non ?

Entre nous, les mots de « magie noire » et « espionnage » sont prononcés. Sur Internet, les rumeurs les plus folles circulent sur la façon dont cet algorithme plutôt intrusif fonctionnerait.

- Il existerait un « profil fantôme » de chacun d'entre nous, pré-rempli et automatiquement activé dès notre inscription.

3. A noter, on en formule une autre pour se faire peur : facebook nous proposerai aussi les personnes qui nous « stalkent » (espionnent en ligne) ou que nous avons récemment « stalkées ».

Un journaliste du Huffington Post a fait la même hypothèse. Ce que le réseau social a nié avec force.

« Ce serait très dangereux économiquement. Facebook n'est pas une société idiote, elle prend des risques calculés. » Pour lui, l'explication est beaucoup plus simple :

Ah bon ?
Un aspirateur à données via

« Quand on "date" quelqu'un sur Tinder, on lui donne bien son numéro avant, non ? Facebook se connecte en fait à votre répertoire. »
Ah bon ?

On résume. Il faut imaginer l'algorithme de Facebook comme un aspirateur à données géant.



En définissant les réseaux auxquels on appartient, Facebook calcule nos chances de connaître telle ou telle personne. Et il peut même prédire nos futures amitiés. Un peu de probabilités et c'est dans la boîte.

●●○○ Bouygues 40 16:44

Avertissement de Messenger, dont la « synchronisation » permet au contact de « se connecter sur Facebook »

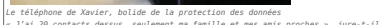
Surtout, depuis qu'il est arrivé sur votre mobile, via les outils Facebook et Messenger, le réseau social a un tas d'autres informations à mettre sous la dent de leur algo : vos contacts téléphoniques et vos mails.

Vous l'avez autorisé, probablement sans en avoir conscience, au moment de l'installation de l'une et/ou l'autre application.

Comme c'était un jour de pluie, j'ai voulu tester la puissance de cet algorithme qui marche donc sur deux pieds :

- Je décide de créer un compte avec un numéro de téléphone et avec un faux nom. Le mien est déjà lié à un compte, donc Facebook le refuse.

Il y a une personne dans ces bureaux qui n'a pas lié son compte Facebook à son numéro. J'ai nommé : Xavier de La Porte. Il possède un charmant Nokia cassé sur le dessus.



Il n'est évidemment pas question d'applications quelconques. Avec le numéro de Xavier, Facebook accepte la création du compte de « Mathilde Machin », 21 ans.



Facebook, après s'être creusé les méninges un moment – c'est un peu technique –, me confirme la dernière hypothèse.

Un algo gourmand

que les rumeurs. Facebook insiste sur le fait que :

- l'algorithme, gentil, ne cherche qu'à vous faire retrouver vos amis et échanger avec eux ;
Facebook ne possède pas et n'utilise pas votre numéro de téléphone. Il s'agit pour vous mettre en relation des profils

- Un samedi soir, vous êtes tombée amoureux d'un ami d'ami. Le lendemain, vous demandez à l'ami commun son numéro. Vous hésitez à envoyer un message, vous bloquez plusieurs jours. Sachez donc que ce mec, à qui vous n'avez rien envoyé, vous a peut-être déjà vu apparaître dans « Vous s'emmêlent les pieds. Vous n'êtes pas faits pour être amis ».



- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphoniques, disques durs, e-mails, courriels, détournements de clientèle...);

[Contact us now](#)

Réagissez à cet article

Quels sont les risque des photos de vos jeunes enfants sur Facebook ?



Une vigilance s'impose et la question à se poser est de savoir comment une photo postée à un instant donné pourrait être perçue X années plus tard sachant que nous ne maîtrisons pas tout quant aux futurs possibles.



Et qui peut la consulter directement ou non. Il convient de savoir si ses amis sont sûrs et de s'assurer de l'identité véridique d'une personne demandant à rentrer en contact avec soi pour éviter les usurpations d'identité potentielles. Facebook et les autres outils – même Snapchat où les courtes vidéos peuvent être récupérées – n'ont rien de journaux intimes. Par ailleurs, il est possible de réserver des comptes pour ses enfants sans les utiliser pour éviter tout conflit avec des homonymes éventuels – certes, Facebook demande que l'on soit majeur numériquement, c'est-à-dire âgé d'au moins 13 ans, mais c'est peu vérifié dans les faits. Mais plus que tout, il convient d'éduquer ses enfants quant au monde numérique et ses pièges en l'étant au préalable soi-même. Un dialogue peut être noué entre enfants et parents mais dans le cadre d'un bébé ou d'un enfant de quelques années, c'est le parent qui est responsable des traces qu'il va léguer à son enfant, d'où une vigilance supplémentaire pour ne pas d'emblée lui entacher sa réputation numérique : photos de l'enfant nu, grimaces, etc. L'utilisation des tags est à manier avec précaution et mieux vaut ne pas reconnaître une personne sur une photo, ce qui fait avant tout le jeu de Facebook ou d'autres outils mais qui n'est pas l'intérêt premier de la personne.

Article de David Fayon. Propos recueillis par Thomas Gorriz



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

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



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Pourquoi vous ne devriez jamais publier de photos de vos jeunes enfants sur Facebook | Atlantico.fr

Facebook regarde dans quels magasins vous faites vos courses



Facebook va désormais traquer les données de ses utilisateurs pour savoir dans quels magasins ils se rendent. Le but est de permettre aux annonceurs de savoir si leurs publicités attirent des consommateurs sur leurs points de vente.



Facebook ne cesse de renforcer son service de publicités. Le réseau social veut proposer une offre plus précise et pertinente pour ses clients. Pour cela, il se servira désormais des données de localisation de ses utilisateurs pour savoir dans quels magasins ils se rendent. Le but ? Permettre aux entreprises de savoir si leurs annonces sur Facebook attirent du monde dans leurs magasins.

Ainsi, les annonceurs pourront comparer le nombre de personnes qui ont vu leurs annonces au taux de fréquentations de leurs points de vente. Ils peuvent également intégrer une carte interactive à leur publicité – sous la forme d’un carrousel – pour indiquer à l’internaute le chemin qui le mènera au magasin le plus proche.

Ces nouvelles fonctionnalités s’inscrivent dans une volonté de Facebook de proposer des services plus personnalisés – et donc plus efficaces – à ses clients. En 2014, la boîte de Mark Zuckerberg avait déjà lancé une plateforme qui permet d’afficher de la publicité aux utilisateurs du réseau social qui se trouvent à proximité du magasin afin de les inciter à s’y rendre rapidement.

Selon Facebook, plusieurs entreprises ont déjà eu l’occasion de tester, en avant-première, ces nouvelles fonctionnalités. Parmi eux, se trouve E.Leclerc. La chaîne de distribution française « a pu atteindre 1,5 millions de personnes dans un rayon de dix kilomètres autour de ses supermarché et a observé qu’environ 12 % des clics sur leur publicité ont entraîné une visite en magasin dans les sept jours qui suivaient », indique Facebook dans son annonce.

Grâce à ces jeux de données très précis, Facebook fournit des outils pertinents pour les entreprises car, grâce à cela, elles peuvent ajuster leur stratégie de communication en fonction de chaque point de vente et de chaque région. Le réseau social prouve encore plus à quel point il représente un atout bien plus puissant que les modes de diffusion traditionnels.

Quant aux utilisateurs de Facebook, si cette information a de quoi énerver, elle n’a rien de vraiment surprenant. Il est de notoriété publique que la publicité ciblée représente le fonds de commerce principal du réseau social. Celui-ci n’est d’ailleurs pas le seul à traquer les internautes pour savoir dans quels magasins ils vont. Google le fait depuis quelques temps déjà, comme le rappelle, dans un tweet, Jason Spero, responsable de la stratégie et des ventes mobiles chez la firme de Mountain View.

Google dispose de données encore plus importantes destinées aux annonceurs et adapte les publicités en fonction, entre autres, des recherches de l’utilisateur et de sa géolocalisation.

Article original de Omar Belkaab



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

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



[Contactez-nous](#)

Réagissez à cet article

Original de l’article mis en page : Facebook regarde dans quels magasins vous faites vos courses – Business – Numerama

Pourquoi vous ne devriez

jamaïs publier de photos de vos jeunes enfants sur Facebook



Atlantico : Poster une photo de son enfant sur Facebook peut-il lui porter préjudice ? Si oui, quand ? Et pourquoi ?



Publier une photo de ses enfants sur Facebook – qui est de loin le leader des réseaux sociaux dans le monde – est un acte compréhensible mais qui fait surtout plaisir sur le moment aux parents. Les parents façonnent l'identité numérique de leurs enfants à l'insu de leur plein gré alors même que le droit à l'oubli n'existe pas sur Internet. Plus tard, certaines traces numériques (photos ou vidéos postées avec les commentaires et tags associés) peuvent être utilisées contre eux surtout si les paramétrages de confidentialités sont mal utilisés.

Et même en postant une photo accessible aux seuls amis, celle-ci peut ensuite être partagée plus largement. En outre les personnes qui vont réagir à la photo permettent de révéler l'écosystème relationnel de la personne. Il est facile d'établir des corrélations entre les personnes. Et en fonction du profil des personnes réagissant de déterminer quel est le profil potentiel de l'enfant sur la photo. Pour les préjudices, on pense avant tout à l'attitude d'un recruteur mais ce peut être aussi des amis potentiels de l'enfant qui le jugeront avec un autre regard. Déjà on google une personne avant de la rencontrer ce qui induit un prisme dans la première rencontre. Le préjudice peut intervenir à des périodes charnières de la vie : adolescence où l'individu se construit et est sensible au regard des autres, entrée dans la vie active, rencontre amoureuse, etc.

Comment fonctionne le système de tag ? Quelle est sa fonction ? Pourquoi l'utilise-t-on ?

Il s'agit d'un système mis en place par Facebook qui permet à un utilisateur de Facebook d'indiquer qu'une personne figure sur une photo. En quelque sorte, un traitement manuel du facebooknaute lui-même vient en complément de l'algorithme mis en place par Facebook pour collecter des données personnelles (en l'occurrence les photos des visages des personnes) de nature à faire grandir la base d'information relative à une personne. Facebook peut avec l'expérience lui-même déterminer les personnes reconnues sur les photos, ce qui est parfois bluffant. Facebook peut ensuite, en fonction des références à d'autres posts, déterminer le cercle probable de personnes autour de celle qui a été taguée. Ceci lui permet de faire des suggestions (par exemple amis que l'on pourrait connaître, voire produits ou services que l'on est susceptible d'aimer car les goûts de ses amis sont souvent plus proches des siens que ceux d'inconnus) avec des taux de retour plus pertinents.

L'objectif de Facebook est d'exploiter le *big data* constitué par les photos et leurs tags pour sans cesse améliorer les résultats pour les marques partenaires et qui paient ses services. Par ailleurs, les algorithmes qui permettent de reconnaître les visages et les techniques de bio-identification ne sont qu'à leur début. Demain, à partir d'une simple photo, il sera, avec des outils idoines, possible de dresser le portrait robot d'une personne en allant fouiller sur l'ensemble de la websphère (pas seulement sur Facebook mais sur l'ensemble des réseaux sociaux et des sites) pour collecter les numéros de téléphone, les adresses mails et d'autres détails personnels associés. Ceci peut présenter des opportunités réelles pour mieux connaître rapidement une personne, mais présente des risques. Des garde-fous et une éthique sont à construire pour éviter que le numérique ne soit un facteur d'exclusion ou un moyen d'ostraciser les internautes. Alors que les États-Unis sont dans le mécanisme d'*opt-out* (utilisation *a priori* des données personnelles sans autorisation préalable), l'Europe préfère l'*opt-in* qui constitue un principe de précaution quant à l'exploitation des données personnelles. Mais force est de constater que les outils majoritairement utilisés en Europe sont Américains et que nous sommes GAFA-dépendant (*Ndlr : GAFA = Google, Apple, Facebook, Amazon*) et qu'en contrepartie de la gratuité d'utilisation d'un service, nous fournissons et souvent avec beaucoup de zèle des données personnelles que ces outils utilisent à la fois avec un traitement automatique et un traitement humain qui le perfectionne comme celui des tags.

Article original de David Fayon 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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Pourquoi vous ne devriez jamais publier de photos de vos jeunes enfants sur Facebook | Atlantico.fr

Pourquoi l'inventeur du Web rêve d'un autre Internet ?



Inventeur du Web il y a plus de 25 ans, Tim Berners-Lee regrette le pouvoir qu'on a pris sur lui les états et les grandes entreprises comme Google ou Facebook. Il souhaite pousser vers un Web plus décentralisé et plus sûr pour ses utilisateurs.



Mais qu'a-t-on fait d'Internet ? C'est la question que se posent régulièrement des pionniers du Web, qui rêvaient de changer le monde et qui l'ont effectivement fait, sans toujours bien savoir si c'est pour le meilleur ou pour le pire. Internet a apporté son lot incontestable d'améliorations dans la vie sociale, en permettant aux citoyens de s'informer davantage, de partager des connaissances et d'entrer plus facilement en contact les uns avec les autres. Mais il est aussi devenu un moyen inédit de surveillance de la population, et une machine libérale qui favorise les plus gros dans une économie plus que jamais mondialisée.

Parmi ceux qui semblent avoir quelques regrets figure l'inventeur du World Wide Web, Tim Berners-Lee. L'homme, qui a créé la première page Web il y a plus d'un quart de siècle, s'est désolé dans le New York Times de ce qu'était devenu en partie Internet. « Il contrôle ce que les gens voient, crée des mécanismes sur la manière dont les gens interagissent. Ce fut génial, mais l'espionnage, le blocage de sites, le détournement du contenu des gens, vous faire aller sur les mauvais sites web... tout ça mine complètement l'esprit d'aider les gens à créer », condamne-t-il.

NOUS N'AVONS PAS UN PROBLÈME TECHNOLOGIQUE, NOUS AVONS UN PROBLÈME SOCIAL

Berners-Lee voit un problème majeur dans le développement du Web qu'il a créé : la possibilité pour les états ou de grandes entreprises de prendre le contrôle et d'imposer leur puissance. Pour les états, il s'agit par exemple de la possibilité qu'ils ont de bloquer l'accès à des sites internet (comme c'est désormais fréquent en France), ou de traquer les communications pour identifier ou géolocaliser des dissidents. Concernant les entreprises, le souci est davantage dans le pouvoir immense que des Facebook ou Google ont sur les populations du monde entier, en étant les principaux vecteurs d'informations, et en glanant des informations de plus en plus précises sur les habitudes et les pensées de chacun.

Pour défendre l'idée de repenser Internet, l'ingénieur a donc participé cette semaine à la conférence Decentralized Web Summit de San Francisco, organisée notamment par la fondation Internet Archive, et des acteurs impliqués dans le bitcoin et la blockchain. Mais il prévient que la solution ne sera pas seulement technique. « Le Web est déjà décentralisé », rappelle-t-il. « Le problème c'est la domination d'un moteur de recherche, d'un grand réseau social, d'un Twitter pour le microblogging. Nous n'avons pas un problème technologique, nous avons un problème social ».

« Nous sommes au bord de découvrir qu'une entreprise peut en arriver au point où en réalité elle contrôlera tout ce que chacun d'entre nous voit », s'était déjà inquiété Berners Lee dans une interview à GeekWire. « Elle décidera des posts de ses amis et des articles de journaux qu'une personne voit, et nous réalisons que nous parlons d'une seule grande multinationale qui a soudainement le contrôle complet sur la perception qu'a quelqu'un de la planète sur laquelle il habite. C'est une bataille constante et nous en sommes très proches tout le temps ».

UN PAIEMENT PLUS FLUIDE POUR UN INTERNET PLUS SAIN

Pour aider à réinventer le Web, Tim Berners-Lee rêve notamment d'un réseau social respectueux de la vie privée des utilisateurs et de leur liberté d'expression. Il est membre du conseil d'administration de MeWe, qui se rêve en Facebook éthique. D'autres technologies décentralisées peuvent aussi aider, comme Tor bien sûr, mais aussi des initiatives comme ZeroNet, qui prétend héberger un Web non censurable en utilisant BitTorrent et du chiffrement, ou MaidSafe, qui utilise aussi une architecture P2P et un système d'échange monétaire baptisé SafeCoin.

À cet égard, Tim Berners-Lee espère aussi voir prospérer un Web où le paiement électronique serait beaucoup plus aisé, et sans intermédiaires à qui verser des commissions (ce qui était à l'origine l'idée du bitcoin, même s'il manque de fluidité dans la validation des transactions). « Imaginez un monde où le fait de payer pour des choses serait facile des deux côtés », demande-t-il, en faisant remarquer que « le modèle publicitaire est le seul modèle pour trop de gens sur le web actuellement ».

Les journaux, par exemple, devraient pouvoir proposer de faire payer quelques centimes pour lire un article, ce qui rapporterait davantage que la publicité, offrirait davantage d'espace d'affichage pour l'information, et éviterait de tracer l'internaute. Or aujourd'hui, le jeu des commissionnements et des empiètements d'intermédiaires fait qu'il est pratiquement impossible d'avoir sur internet la fluidité de paiement offerte par l'argent liquide.

Crédit photo de la une : CC Kristina D.C. Hoepfner

Article original de Guillaume Champeau



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

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



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Pourquoi l'inventeur du Web rêve d'un autre Internet – Politique – Numerama

32 millions de mots de passe Twitter dérobés

 Denis JACOPINI vous informe	32 millions de mots de passe Twitter dérobés
---	---

Après LinkedIn, MySpace et Tumblr, Twitter a lui aussi été victime d'un piratage massif. 32,8 millions de comptes seraient affectés.



Une nouvelle fuite de données pour un réseau social. Un hacker russe affirme avoir dérobé 379 millions d'adresses email et de mots de passe non chiffrés associés à des comptes Twitter. Identifié sous le pseudonyme Tessa88, il aurait mis en vente la base de données en question sur VK, le Facebook russe. LeakedSource, qui a révélé l'information, estime que 32,8 millions de comptes seraient effectivement compromis, une fois les doublons éliminés.

«Nous sommes convaincus que ces noms d'utilisateurs et les identifiants n'ont pas été obtenus par une violation des données Twitter. Nos systèmes n'ont pas été hackés», a déclaré un porte-parole de Twitter. La base de données serait donc le fruit d'une campagne de malware ciblant les particuliers pour récupérer leurs mots de passe.

Sollicité par Techcrunch, Troy Hunt, le fondateur de site haveibeenpwned.com qui permet de voir si une adresse mail fait partie d'une base de données piratée, émet des doutes par rapport à l'authenticité des données piratées: «Les piratages de comptes que nous avons vus jusqu'à présent sont très probablement le résultat de la réutilisation de données issues d'autres piratages», indique-t-il.

Une incitation de plus à modifier son mot de passe

Si Leakedsource propose de vérifier si vos identifiants et mots de passe sont dans leur base et de les retirer gratuitement, le plus simple reste encore de modifier son mot de passe.

Twitter a suggéré au passage de le complexifier, en suivant ses recommandations.

7 Juin



Twitter Support

@Support

To help keep people safe and accounts protected, we've been checking our data against what's been shared from recent password leaks.

Suivre



Twitter Support

@Support

Any time is a good time to make sure your account is secure, starting with an updated password. More tips <https://support.twitter.com/articles/76036>

00:36 – 7 Juin 2016



Safe Tweeting: the basics

Keeping your account secure We want Twitter to be a safe and open community. This help page provides some information and tips to help you practice safe Tweeting and keep your account secure.

support.twitter.com

-
-
- 128128 Retweets
-
- 170170 j'aime

Selon la liste des données divulguées, bien trop de mots de passe restent basiques et facilement trouvables. 123456 prend la première place du podium, suivi de 123456789, qwerty et du classique password.

Ce piratage suit celui de MySpace, de Tumblr et de LinkedIn. 100 millions de mots de passe du réseau professionnel récupérés en 2012 ont été mis en vente mi-mai. Ce piratage avait valu à Mark Zuckerberg, adepte du mot de passe unique «dadada», de voir ses comptes Twitter et Pinterest piratés.

Article original

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 03941 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 ;



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Un hacker russe prétend avoir dérobé des millions de mots de passe Twitter