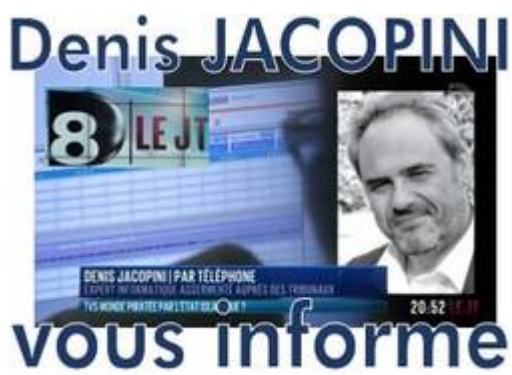
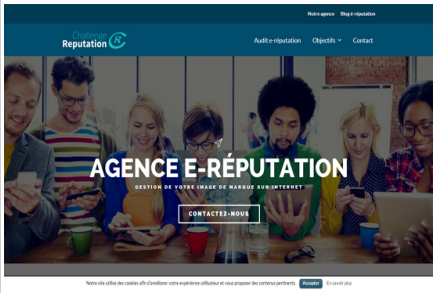
Astuces pour une meilleure gestion de l’e-réputation – Annuaire +1 Annuaire +1



Astuces pour une meilleure gestion de l’e-réputation – Annuaire +1 Annuaire +1

L’e-réputation ne concerne plus les entreprises et les organisations de marque. Tout le monde peut disposer d’une image sur internet. En effet, avec ou sans permission, des sujets peuvent parler d’une personne notamment via des discussions, des images ou des vidéos. Or, dans ces discours et mauvaises appréhensions ne restent pas dans le monde virtuel. En fait, cela peut impacter la vie quotidienne, détruire des relations et même des carrières professionnelles. Heureusement que ce n’est pas une fatalité. L’e-réputation peut être géré et même utilisé à bon escient. Comment faire ?



Ajouter de l’importance à son image
Quels que soient les documents ou fichiers qu’il faut mettre en ligne, il faut les prendre en conscience. CV, photos ou des commentaires faits sur les plateformes sociales, ils contribuent tous à l’e-réputation d’une personne. Bien que quelque peut inévitable, ces contenus sont les vitrines d’une personne, alors autant qu’elle lui ressemble. La meilleure façon est de ne jamais négliger son e-réputation. Tout ce qui est sur internet reste sur internet ! Telle est la règle.

Avoir un bon aspect de l’état des lieux
Le mieux est d’évaluer son e-réputation le plus tôt possible. C’est très simple, il n’y a pas besoin de faire appel à une agence e-réputation pour avoir une idée de son e-réputation. Pour ce faire, il suffit de taper une requête sur la barre de recherche des moteurs de recherche. De porter une analyse sur au moins les deux premières pages (au lieu de rester sur la première). La suite consiste à vérifier s’ils coïncident avec l’image voulue, s’ils peuvent être lus publiquement…

Penser à son avenir
Les réseaux sociaux constituent en fait une bonne alternative pour constituer un réseau professionnel. Il y a également les sites dédiés avec qui, il faut prendre à l’avance des précautions. En fait, pour une candidature donnée les recruteurs ne s’arrêtent pas sur leur site. Ils peuvent étendre (et c’est bien compréhensible) leur recherche sur les autres plateformes sociales et même sur la totalité des moteurs de recherche.
De même pour les amis Facebook par exemple, ce sont les personnes les plus susceptibles de devenir un danger pour un internaute. La situation n’est pas toujours délibérément provoquée, par contre une identification sur une photo relatant une soirée vertigineuse entre élève et prof employer et employeur ne fait pas bon ménage. Pour éviter cette situation, il est indispensable de bien maitriser les paramètres (ce que peu de gens font également).
Après les constatations, les actions ! Quelle que soit la plateforme, il faut toujours vérifier les paramètres. Entreprendre des petites actions peut permettre à aider des problèmes plus graves. Comme le classement des amis par rapport au lien et relation partagée. Par exemple pour Facebook, cliquer sur rubrique confidentialité et choisir option « examiner les publications dans lesquelles vos amis vous identifient avant qu’elles n’apparaissent sur votre journal ».

Apparaitre ou ne pas apparaitre ?
Telle est la question ! En premier lieu, demander le droit de ne faire aucune publication sur internet ! C’est toujours possible à faire, mais il faut prendre en compte les autres internautes qui peuvent toujours influer l’e-réputation. L’inconvénient réside alors dans le fait qu’il n’y aura que du mauvais contenu à l’encontre de la personne en question. Un autre inconvénient est que les recruteurs n’aiment pas trop les candidats qui sont trop discrets sur le web.
Du coup, autant prendre le mal par les cornes ! Avoir le pouvoir de supprimer les contenus indésirables en contactant Google ou en faisant appel à une agence e-réputation.

Réagissez à cet article

Source : *Astuces pour une meilleure gestion de l’e-réputation – Annuaire +1 Annuaire +1*

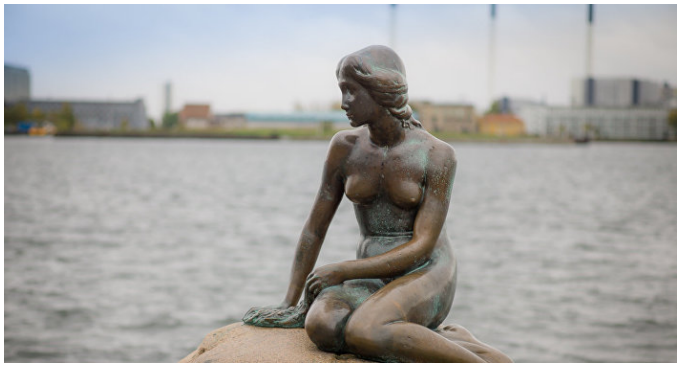
Le « friend finder » de Facebook devient illégal en

Allemagne

Le « friend finder » de Facebook devient illégal en Allemagne

La plus haute cour de justice allemande a déclaré illégal l'outil de recherche d'amis « friend finder » du réseau social américain Facebook.

Le comité de la Cour fédérale d'Allemagne a jugé que la fonction de recherche d'amis de Facebook viole la loi sur la publicité, a rapporté le journal britannique The Guardian.



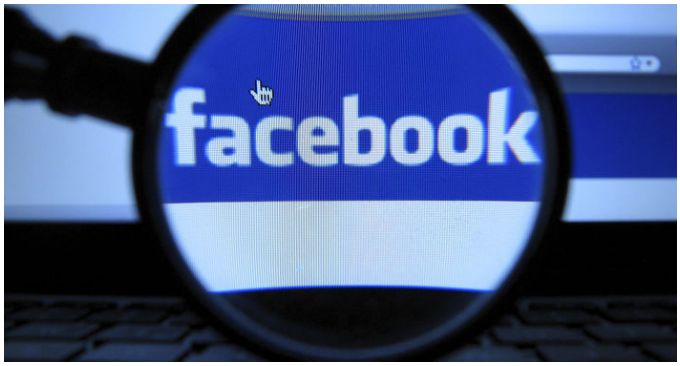
© FLICKR/ MOMPL

Facebook: cachez-moi cette sirène que je ne saurais voir!

En accédant au carnet d'adresses de l'utilisateur, le « friend finder » récolte tous les contacts et leur envoie des invitations leur proposant de s'inscrire sur le réseau social. C'est ce mécanisme de collecte d'adresses électroniques et son utilisation dans un but marketing qui a été condamné.

La cour a conclu que cette pratique de marketing était trompeuse, confirmant les décisions de deux tribunaux de Berlin de 2012 et 2014, qui avaient constaté que Facebook violait les lois allemandes sur la protection des données et sur les pratiques commerciales déloyales.

La Cour fédérale a également déclaré que Facebook n'avait pas informé d'une façon adéquate les membres du réseau sur le mécanisme qui utilise les données de leurs contacts.



© AP PHOTO/ DAPD, JOERG KOCH

Facebook dévoile les sujets de discussion les plus populaires en 2015

Le représentant officiel de Facebook en Allemagne a, à son tour, déclaré que la société attendait le rapport explicatif de la décision finale et qu'elle l'étudierait les solutions « pour évaluer tout impact sur les services ».

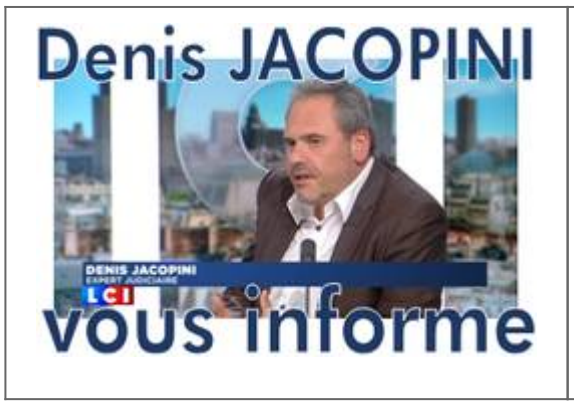
C'est une vraie victoire pour l'association de protection des consommateurs allemands VZBV (Verbraucherzentrale Bundesverband) qui menait ce combat depuis 2010. En outre, elle ne compte pas arrêter sa lutte contre les géant d'Internet et souhaite maintenant vérifier les mécanismes de LinkedIn et Twitter.

« En plus de Facebook, d'autres services utilisent cette forme de publicité pour attirer de nouveaux utilisateurs. Ils doivent maintenant probablement repenser leurs systèmes », a déclaré Klaus Mueller, président de VZBV.

Réagissez à cet article

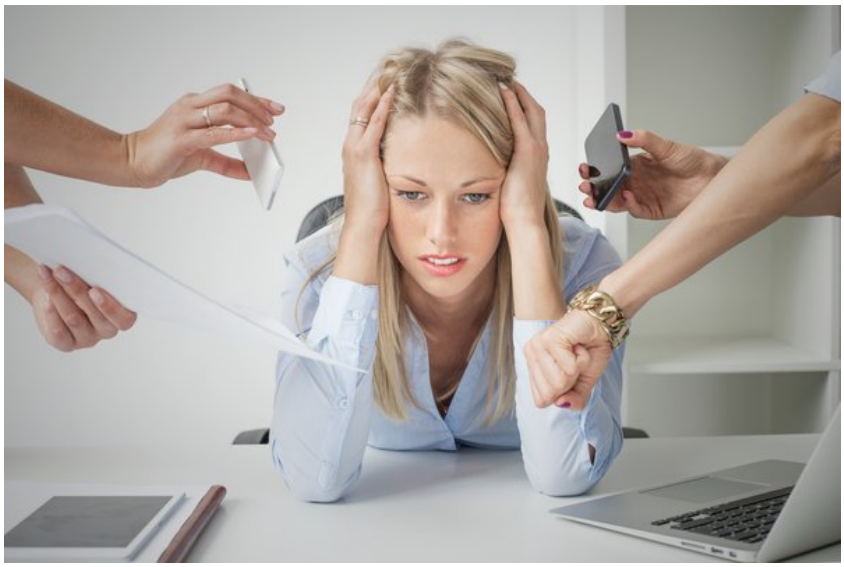
Source : *Le « friend finder » de Facebook devient illégal en Allemagne*

Utiliser Internet à des fins personnelles peut être un motif de licenciement



Utiliser Internet à des fins personnelles peut être un motif de licenciement

La justice européenne confirme à nouveau que dans un cercle professionnel, la direction a un droit de regard sur les échanges électroniques des salariés. Les e-mails ou autres services de communication en ligne peuvent être surveillés.



La Cour européenne des droits de l'homme (CEDH) vient de débouter un plaignant dont le licenciement avait été motivé par une utilisation indue de ressources professionnelles. Ce dernier avait utilisé à des fins personnelles, et pendant les heures de travail, des outils professionnels mais également la connexion de l'entreprise, entre autres services en ligne.
Le plaignant, un ingénieur roumain en charge des ventes, utilisait en particulier Yahoo Messenger pour converser avec des clients mais surtout avec des connaissances personnelles. La décision de la Cour met ainsi en avant le fait que l'employé échangeait très régulièrement des messages « avec son frère et sa fiancée et portant sur des questions personnelles telles que sa santé et sa vie sexuelle ».
La société a mis fin au contrat de son collaborateur au motif que son règlement intérieur interdisait l'usage de ces mêmes ressources à des fins personnelles. Cet argument a été soutenu par la justice d'autant qu'elle ne qualifie pas d'abusif le fait qu'un employeur souhaite vérifier que ses employés accomplissent leurs tâches professionnelles pendant les heures de travail.

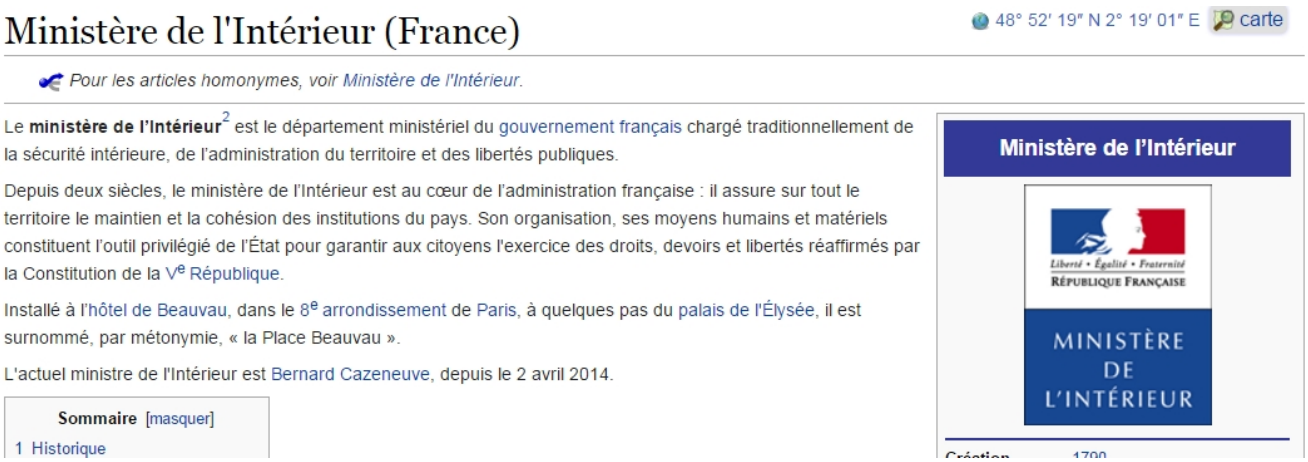
Stress travail e-mail email

La CEDH estime donc que la surveillance des communications du salarié était légitime dans la mesure où elle est considérée comme raisonnable. Cela signifie que l'employeur a cherché à préserver la productivité de ses salariés sans pour autant instaurer de politique rigide de surveillance des communications. La Cour précise que cette attention portée à l'encontre du collaborateur était organisée dans le cadre d'une procédure disciplinaire.
En France, le régime est très similaire. La justice valide régulièrement des licenciements lorsque des salariés utilisent trop souvent leurs outils informatiques pour des motifs personnels. Il est en général question de navigations régulières et conséquentes pour des tâches qui ne sont en rien en rapport avec le travail.

Réagissez à cet article

Source : *Utiliser Internet à des fins personnelles peut être un motif de licenciement*

Wikipédia bloque pour un an le ministère de l'Intérieur pour « foutage de gueule »



Ministère de l'Intérieur (France)

48° 52′ 19″ N 2° 19′ 01″ E carte

Pour les articles homonymes, voir Ministère de l'Intérieur.

Le **ministère de l'Intérieur**[2] est le département ministériel du gouvernement français chargé traditionnellement de la sécurité intérieure, de l'administration du territoire et des libertés publiques.

Depuis deux siècles, le ministère de l'Intérieur est au cœur de l'administration française : il assure sur tout le territoire le maintien et la cohésion des institutions du pays. Son organisation, ses moyens humains et matériels constituent l'outil privilégié de l'État pour garantir aux citoyens l'exercice des droits, devoirs et libertés réaffirmés par la Constitution de la Ve République.

Installé à l'hôtel de Beauvau, dans le 8e arrondissement de Paris, à quelques pas du palais de l'Élysée, il est surnommé, par métonymie, « la Place Beauvau ».

L'actuel ministre de l'Intérieur est Bernard Cazeneuve, depuis le 2 avril 2014.

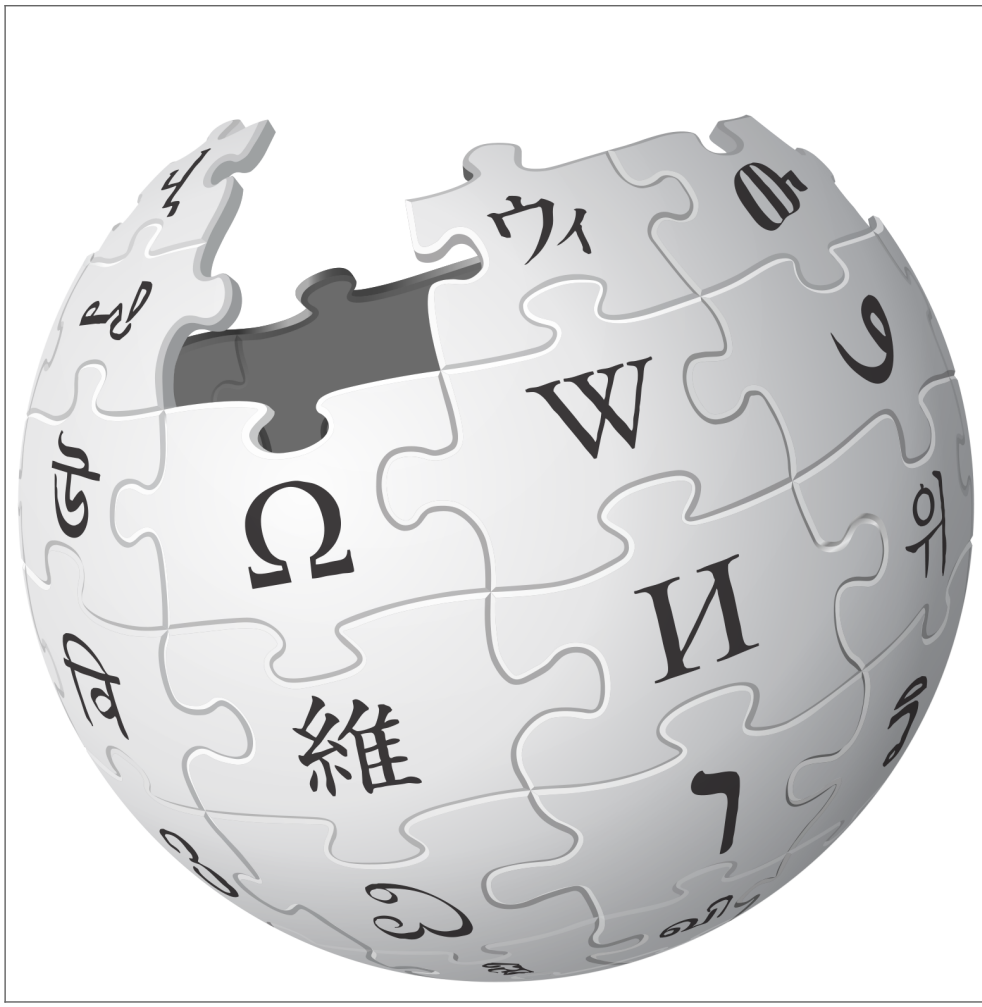
Sommaire [masquer]

1 Historique

Ministère de l'Intérieur

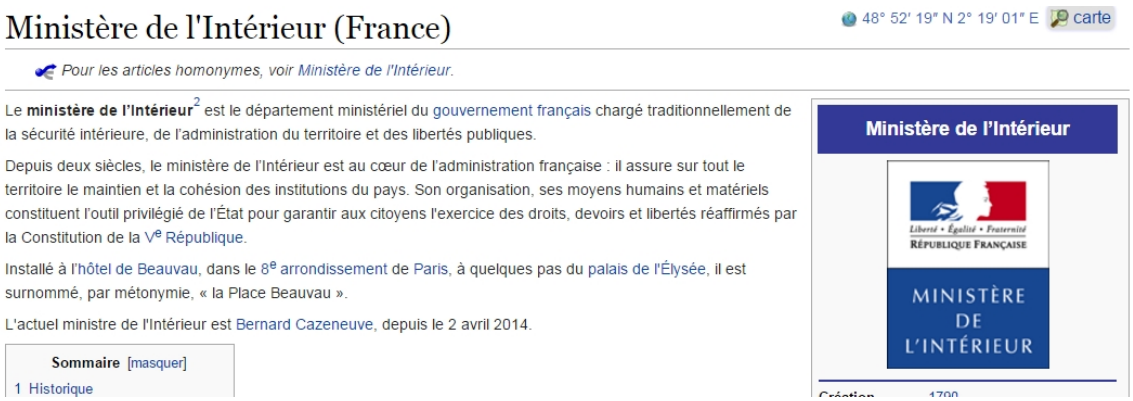
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR



Wikipédia bloqué pour un an : le ministère de l'Intérieur pour « foutage de gueule »

Le ministère de l'Intérieur a visiblement eu la main un peu lourde quant au nombre de modifications apportées sur sa page Wikipédia, mais est également accusé de différents dérapages. Résultat : un an de blocage.



Ministère de l'Intérieur (France)

48° 52′ 19″ N 2° 19′ 01″ E carte

Pour les articles homonymes, voir Ministère de l'Intérieur.

Le **ministère de l'Intérieur**[2] est le département ministériel du gouvernement français chargé traditionnellement de la sécurité intérieure, de l'administration du territoire et des libertés publiques.

Depuis deux siècles, le ministère de l'Intérieur est au cœur de l'administration française : il assure sur tout le territoire le maintien et la cohésion des institutions du pays. Son organisation, ses moyens humains et matériels constituent l'outil privilégié de l'État pour garantir aux citoyens l'exercice des droits, devoirs et libertés réaffirmés par la Constitution de la Ve République.

Installé à l'hôtel de Beauvau, dans le 8e arrondissement de Paris, à quelques pas du palais de l'Élysée, il est surnommé, par métonymie, « la Place Beauvau ».

L'actuel ministre de l'Intérieur est Bernard Cazeneuve, depuis le 2 avril 2014.

Sommaire [masquer]

1 Historique

Ministère de l'Intérieur

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

Création 1790

Une interdiction de contribuer délivrée pour cause de « foutage de gueule ». Cela prêterait à sourire si le blocage en question ne concernait pas le ministère de l'Intérieur. D'après le Canard enchaîné, l'encyclopédie en ligne a en effet bloqué l'adresse IP de la place Beauvau pour « attitude non collaborative », « passage en force » et « foutage de gueule ».

En plus de modifications trop nombreuses à son goût, Wikipédia accuse également les fonctionnaires de vandalisme répété. Le 21 août dernier, Wikipédia a remarqué un changement sur sa page de présentation, avec la sympathique mention « Sale batar » (avec la faute). La modification émanait de l'adresse IP du ministère.

Début décembre, l'encyclopédie en ligne avait adressé un « dernier avertissement » à l'encontre du compte du ministère : visiblement, cela n'a pas suffi.

Wikipedia Beauvau

Après un premier blocage temporaire en 2013 (la fiche du préfet de police de l'époque, Bernard Boucault, avait subi six modifications en 30 minutes afin d'effacer la trace de ses démêlés avec les opposants au mariage pour tous), le compte du ministère de l'Intérieur se retrouve désormais bloqué pour un an. Difficile de comprendre comment, au sein d'un ministère, de tels agissements peuvent se répéter.

Toujours est-il qu'il y a fort à parier que ce dernier trouvera tout de même les moyens de contrôler ce qui se passe sur sa page de référence.

Réagissez à cet article

Source : *Wikipédia bloque pour un an le ministère de l'Intérieur pour « foutage de gueule »*

Les 5 dangers pour vos ordinateurs, smartphones et données en 2016

Les 5 dangers pour vos ordinateurs, smartphones et données en 2016

Les 5 tendances qui motiveront leurs actions envers votre ordinateur, votre smartphone, vos données…

Ecartelée entre la démocratisation de l'Internet des objets (thermostat intelligent, balance connectée…), la prise de pouvoir du stockage dans le « cloud » et l'émergence des nouveaux smartphones vedettes, la sphère des nouvelles technologies subira en 2016 les assauts des virus virulents, des arnaques en ligne, des cybercriminels.
Comme un caméléon virtuel, la cybercriminalité s'adaptera plus que jamais à l'air du temps pour exploiter les nouveaux territoires en friche.
Entre prudence et clairvoyance, voici les 5 tendances cybercriminelles qui se développeront ces 12 prochains mois, selon les experts de l'éditeur de solution de sécurité BullGuard.

1. La montée en puissance du « ransomware »
Impitoyable méthode d'extorsion, le « ransomware » bloque votre ordinateur, crypte vos fichiers personnels et vous réclame un paiement en ligne pour les libérer.
La menace brandie en cas de refus de payer la rançon : l'extermination de vos données (photos, vidéos, documents…).
Alors que les virus à l'ancienne et les chevaux de Troie accusent une certaine perte de vitesse, le « ransomware » est appelé à les dribbler.
Ces logiciels malveillants s'attrapent en visitant un site préalablement « hacké » (piraté) ou un obscur site volontairement malveillant, en téléchargeant des fichiers vérolés, notamment sur les plateformes d'échange de fichiers illégaux…

2. Le smartphone, cette cible indiscrète
Connecté à Internet 7 jours sur 7, 24 heures sur 24 dans le scénario le plus extrême, le smartphone concentre une myriade de données personnelles, des adresses email de vos contacts au numéro de votre carte de crédit.
Le téléphone est par conséquent une cible de choix pour les cybercriminels, qui rivalisent d'ingéniosité pour contourner les nouvelles barrières de sécurité régulièrement déployées par Apple pour ses iPhone et Google pour son système d'exploitation mobile Google Play.
Après avoir concentré leurs efforts sur la Chine et l'Extrême-Orient, les cybercriminels devraient viser tout particulièrement l'Europe en 2016.
Certes, nos smartphones étaient déjà menacés par le virus et les logiciels malveillants. Hélas, le niveau d'alerte devrait grimper de quelques degrés.

3. L'Eldorado inquiétant de l'Internet des objets
Nouvelle marotte des constructeurs, l'Internet des objets entend envahir notre quotidien pour évaluer et prédire nos besoins, mesurer notre activité, adapter l'éclairage et le chauffage de notre habitation en fonction de nos usages…
Qu'il s'agisse d'un pèse-personne connecté ou d'un thermostat intelligent, ces appareils vulnérables de par leur connexion constante à Internet récoltent au kilo les données personnelles.
Imaginons le cas d'une caméra de sécurité connectée. Elle pourrait simplement être détournée par un cybercriminel pour détecter les moments où vous quittez votre maison.
Toujours en quête d'un standard, notamment pour la sécurité, la galaxie de l'Internet des objets, tout juste née de son Big Bang historique, ne manquera pas de révéler en 2016 ses failles et ses vulnérabilités.

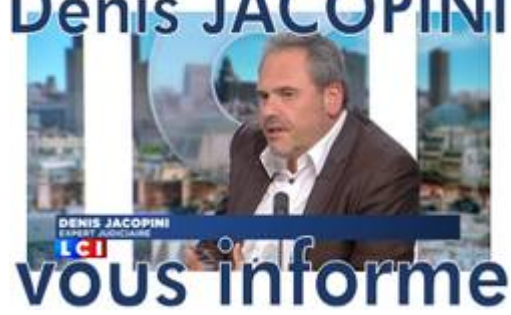
4. Des nuages dans le ciel du « cloud »
Inexorable lame de fond qui modifiera à jamais le monde du stockage, le « cloud » éparpille données et fichiers dans un nuage de serveurs (ordinateurs) répartis dans d'immenses « data center » aux quatre coins du monde.
Ces « fermes » informatiques dédiées au stockage et au traitement des données présentent un double intérêt pour les cybercriminels.
Leur puissance peut être détournée à d'autres fins, tandis que les données stockées constituent un sérieux trésor de guerre au cœur duquel il est tentant de piocher.
Objet de toutes les attentions des esprits mal intentionnés, la vulnérabilité du « cloud » risque d'être régulièrement soulignée ces prochains mois.

5. Les gangs sous les projecteurs
Les cybercriminels se structurent en gangs d'une efficacité redoutable, souligne BullGuard.
« Ils passent des semaines, voire des mois, à effectuer des missions de reconnaissance avant d'attaquer des organisations », témoignent les experts de l'éditeur. « Ces entreprises ont été conçues dès le départ pour se spécialiser dans les crimes informatiques et ont des hiérarchies cloisonnées qui incorporent des programmeurs spécialisés dans le piratage, de vendeurs de données et des gestionnaires, tous supervisés par un cadre supérieur. Ces équipes de cybercriminels occuperont le devant de la scène en 2016. »

Réagissez à cet article

Source : *Virus, arnaques en ligne, cybercriminalité : les 5 dangers de l'année 2016 – L'Avenir Mobile*

Et si les fuites de données sur Réseaux sociaux venaient de vos voisins ?

	Et si les fuites de données sur Réseaux sociaux venaient de vos voisins ?

Selon une étude de l'université de Penn State aux Etats-Unis, les utilisateurs de réseaux sociaux se soucieraient bien moins de livrer des informations privées sur leur liste d'amis que de divulguer les leurs.

Quel internaute n'a jamais utilisé une application externe à Facebook qui demande d'accéder à sa date de naissance, à ses photographies et même aux informations personnelles de ses amis ? Les développeurs qui créent des applications tierces à lancer à partir des plateformes de réseaux sociaux demandent régulièrement l'accès à des données privées pas toujours nécessaires. En revanche, elles peuvent être revendues et cela constitue une source financière non négligeable pour ces développeurs.
Mais qu'en est-il des internautes ? A combien jugent-ils la valeur de leurs informations personnelles, et considèrent-ils la vie privée de leurs amis aussi précieuse que la leur ?

Révélée le 14 décembre dernier lors de l'International Conference on Information Systems au Texas, une étude montre que les internautes sont plus soucieux de leurs données privées que de celles de leurs amis. En effet, lorsqu'on leur demandait d'évaluer en dollars la valeur de leurs propres informations quand une application tierce en avait besoin pour pouvoir fonctionner, la moyenne était de $2.31, alors que celles de leurs amis étaient évaluées à $1.56.
Les réseaux sociaux fonctionnent le plus souvent sur le modèle de l'interconnexion des données pour créer de la valeur. La vie que l'utilisateur affiche et qu'il veut voir rester privée est donc intrinsèquement liée à la confidentialité des informations des autres. A noter qu'en avril 2015, la société Facebook, régulièrement attaquée pour sa politique d'utilisation des données d'utilisateurs, a annoncé de sérieuses restrictions quant aux informations demandées par des applications tierces.

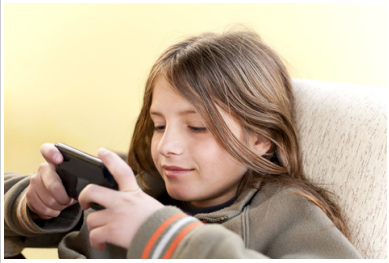
Réagissez à cet article

Source : *Réseaux sociaux : les données du voisin valent moins | L'Atelier : Accelerating Business*

À partir de quel âge peut-on laisser les ados s’inscrire sur les réseaux sociaux ?

À partir de quel âge peut-on laisser les ados s’inscrire sur les réseaux sociaux ?

Les réseaux sociaux seront-ils bientôt interdits aux moins de 16 ans ? La nouvelle législation européenne sur la protection des données, approuvée le 17 décembre, entend relever l'âge minimum pour pouvoir s'inscrire sans consentement parental.



Bruxelles prévoit d'interdire l'accès aux réseaux sociaux aux adolescents de moins de 16 ans, qu'en est-il exactement ?

Pour le moment, il s'agit d'un accord de principe qui devra être soumis au vote du Parlement européen en 2016. Rien n'est donc fait. Cette disposition, ajoutée à la dernière minute au texte sur la protection des données personnelles, fixe à 16 ans l'âge minimum pour s'inscrire sur les réseaux en ligne. Mais chaque État peut ensuite déterminer ses propres limites entre 13 ans et 16 ans.

La règle n'est pas très contraignante, mais c'est tout de même un progrès puisque, à ce jour, aucune loi française ne fixe l'âge d'utilisation pour les mineurs. Actuellement, nous appliquons le droit américain avec la loi COPPA (Children's Online Privacy Protection Act) qui interdit aux sites de recueillir des données d'enfants de moins de 13 ans, sans consentement parental. Si outre-Atlantique, celle-ci est très contraignante, ce n'est pas le cas en France. Les jeunes peuvent s'inscrire en mentant sur leur âge sans conséquences.

À partir de quel âge peut-on les laisser s'inscrire ?

En dessous de 13 ans, ce n'est pas souhaitable car les enfants ne font pas la différence entre vie publique et vie privée. À partir de 13 ou 14 ans, en revanche, ils commencent à acquérir un esprit critique qui leur permet de prendre un peu de recul. Mais la question n'est pas tant l'âge auquel il faut les laisser s'inscrire sur les réseaux sociaux que celui auquel on leur donne un smartphone. Ces petits joujoux sont des réseaux sociaux à eux tout seuls, avec les SMS. Ils donnent en outre accès à tous les sites Internet. Or, la plupart des parents ne pensent pas à installer un contrôle parental.

Il faut donc retarder le plus possible l'acquisition du smartphone, à la fois pour protéger l'enfant des contenus inappropriés et pour qu'il comprenne qu'on peut s'en passer. Un tiers des élèves de CM1-CM2 que je rencontre lors de mes interventions dans les établissements scolaires possède un smartphone. Difficile dans ces conditions de ne pas devenir dépendant.

Smartphone ou ordinateur, comment accompagner les adolescents sur les réseaux sociaux ?

Il faut commencer par installer un contrôle parental, quel que soit le terminal. Les parents doivent ensuite expliquer à l'adolescent la stratégie de ces sites Internet qui revendent les données personnelles à des fins publicitaires. Les contenus sont gratuits, mais l'utilisateur devient en quelque sorte un produit commercial. Une fois cette dimension abordée, il faut l'accompagner dans la phase d'inscription en regardant avec lui les différents paramètres du site. Ainsi, il est primordial de limiter l'accès aux publications aux seuls amis, de même qu'il ne faut pas accepter d'inconnus ou de simples connaissances dans son réseau. Il est également essentiel de rappeler à l'adolescent qu'une fois en ligne, les contenus ne peuvent plus être supprimés, ou alors au prix de démarches complexes sans aucune garantie, puisque n'importe qui peut en faire une copie.

Certains réseaux sociaux sont un peu plus encadrés que d'autres. C'est le cas de Facebook, Instagram et WhatsAPP (qui appartiennent au premier) ainsi que Twitter. En revanche, je déconseille fortement Snapchat. Cette application, qui permet d'échanger des photos de manière instantanée et soi-disant éphémère, est beaucoup plus incontrôlable. Quel que soit le site ou l'application, les parents doivent toujours accompagner les adolescents et, a fortiori, les enfants dans l'univers numérique… comme ils le ferraient dans la rue ou sur la route.

Réagissez à cet article

Source : *À partir de quel âge peut-on laisser les ados s'inscrire sur les réseaux sociaux ? | La-Croix.com – Actualité*

L'histoire interdite du piratage informatique (Documentaire)

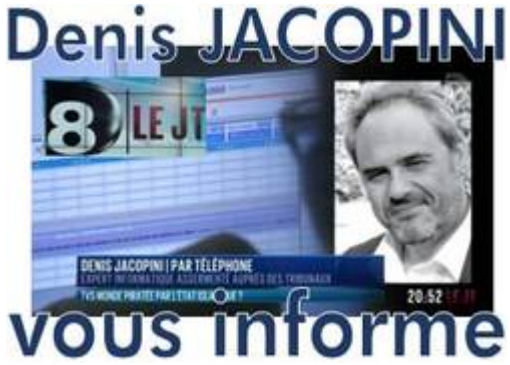
L’histoire interdite du piratage informatique (Documentaire)

Hacker
C’est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.
Aujourd’hui ce mot est souvent utilisé à tort pour désigner les personnes s’introduisant dans les systèmes informatiques.

Réagissez à cet article

Source : *[Documentaire] L’histoire interdite du piratage informatique – TrLoad.net | Download Info | Video | Global Music Video | Top Videos, Artist, Songs, Free Mobile Music Download*

Arnaques et usurpation de vos données personnelles sur internet au Burkina Faso



Arnaques et usurpation de vos données personnelles sur internet au Burkina Faso

Face à la multiplication des plaintes pour piratage de comptes mails, usurpation d'identités sur les réseaux sociaux, Facebook notamment, suivi d'arnaques ou de chantage, enregistrées par la Commission de l'Informatique et des Libertés (CIL), il me plaît de rappeler quelques bonnes pratiques à adopter pour éviter de tomber dans le piège des cyberdélinquants.

Ainsi, il convient de prendre les précautions suivantes :

• Ne pas répondre à un courrier électronique (mail) ou à un message dans lequel votre mot de passe, votre adresse mail, votre numéro de compte bancaire, etc. sont demandés pour quelque raison que ce soit ;

• Eviter de saisir ou communiquer ses informations personnelles confidentielles (mot de passe, coordonnées financières…) sur un ordinateur dont on n'a pas l'assurance qu'il est sécurisé ;

• Eviter d'accepter les invitations d'inconnus sur les réseaux sociaux, Facebook notamment ;

• Eviter d'échanger des contenus inappropriés (photos, vidéos intimes) sur les réseaux sociaux en général et sur Facebook en particulier ;

• Eviter de se connecter aux réseaux internet public (wifi ouvert, des aéroports, des salles de conférences…) ;

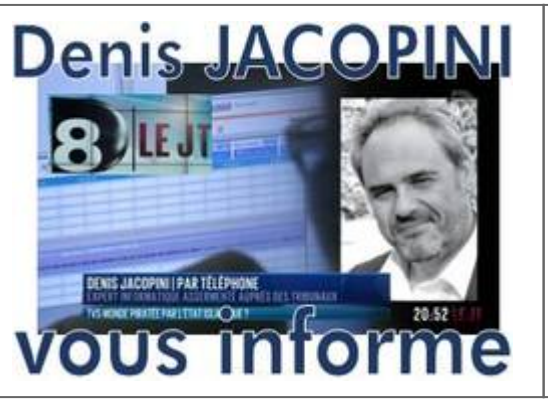
• Utiliser un logiciel anti-virus, activer le pare-feu pour un minimum de protection de vos ordinateurs personnels, veiller à leurs mises à jour.

La protection de vos données personnelles, notre préoccupation.
LA PRESIDENTE

Réagissez à cet article

Source : *Arnaques et usurpation de vos données personnelles sur internet : conseils (…) – leFaso.net, l'actualité au Burkina Faso*

La CNIL demande à Facebook de ne pas tracer les non-membres



La CNIL demande à Facebook de ne pas tracer les non-membres

À la suite du jugement belge exigeant de Facebook qu'il mette fin au pistage des internautes, cinq autorités de protection de la vie privée demandent au réseau social d'appliquer les conséquences du verdict sur l'ensemble de l'Union européenne.

Dans son bras de fer contre Facebook, qui est accusé de suivre tous les internautes à la trace, y compris ceux qui ne sont pas inscrits sur le réseau social, la commission de la protection de la vie privée belge n'est pas seule. L'institution peut en effet compter sur le soutien de quatre autres autorités européennes.

Celles-ci ont en effet publié une déclaration commune qui réclame la fin de l'ingérence du site américain dans la vie privée des internautes. Ce texte fait suite au jugement rendu en première instance par le tribunal civil de Bruxelles, qui condamne Facebook à cesser de tracer l'activité des internautes en Belgique lorsqu'ils visitent des sites web sur lesquels sont installés des boutons de partage, comme le célèbre « J'aime ».

Les autorités de France, de Belgique, d'Espagne, des Pays-Bas et de Hambourg sur la même ligne.

« Tout en reconnaissant le droit de Facebook à faire appel de ce jugement, le Groupe de contact attend de la société qu'elle se conforme à ce jugement sur tout le territoire de l'Union européenne », écrivent-elles. Elles ajoutent, dans un communiqué, que cette immixtion « n'est pas acceptable » et que Facebook doit « prendre les mesures nécessaires pour se mettre en conformité » avec les règles communautaires.

Mais en la matière, les mesures que Facebook a déjà déployées pour respecter le jugement de la justice belge ont eu pour effet d'irriter la commission de la protection de la vie privée belge. En effet, au lieu de neutraliser le cookie litigieux (intitulé « datr » et que Facebook justifie au nom de la sécurité de ses membres), le réseau social a préféré bloquer l'accès aux internautes belges qui ne sont pas connectés au service.

Réagissez à cet article

Source : http://www.numerama.com/politique/133980-la-cnil-demande-a-facebook-de-ne-pas-tracer-les-non-membres.html