La double authentification de Google contournée par des hackers

La double authentification de Google contournée par des hackers

Alors que la double authentification semblait être la meilleure solution pour protéger les données personnelles des internautes, voilà que celle de Google a réussi à être contournée par des pirates. Autrement dit, les spécialistes de la sécurité vont encore devoir se creuser la tête pour trouver encore mieux !

La double authentification plombée par des pirates ?

Puisque la double identification implique qu'un utilisateur saisisse un mot de passe puis qu'il confirme son identité en saisissant un code préalablement reçu par SMS afin de pouvoir accéder à ses comptes, elle semblait être une solution fiable pour bien protéger les données des internautes.

Mais ça, c'était avant puisque des pirates ont réussi à contourner la double authentification de Google pour accéder aux comptes d'utilisateurs tiers.

Pour ce faire, les hackers ont mis en place une méthode plutôt astucieuse. En effet, s'ils disposent de l'adresse mail et du mot de passe, ils se font passer pour la firme de Mountain View, expliquent qu'une activité suspecte a été repérée et invitent l'utilisateur à renvoyer le code de sécurité qui leur a été envoyé.

Sans le savoir, les utilisateurs fournissent alors la clé de l'ultime protection aux pirates qui ont désormais le temps de commettre tous les actes malveillants qui désirent.

Une porte d'entrée vers les terminaux mobiles des utilisateurs ?

En s'offrant un accès aux comptes de messagerie des internautes, les pirates s'offrent une vraie porte d'entrée vers les terminaux mobiles de leurs propriétaires.

En effet, s'ils contrôlent le compte mail de leurs victimes, ils pourront facilement envoyer des mails sur Gmail incluant des pièces jointes frauduleuses qui peuvent être des applications malveillantes. Si le mail est ouvert depuis le mobile, le terminal sera alors automatiquement infecté.

Autrement dit, le hacker pourra avoir un accès complet à l'ensemble des données qu'il contient.

Incontestablement, la double authentification a donc ses limites…

Article original de Jérôme DAJOUX

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

Original de l’article mis en page : La double authentification de Google contournée par des hackers

---

Les dirigeants sont les premiers responsables en cas de cyberattaques subies par leur entreprise

	Les dirigeants sont les premiers responsables en cas de cyberattaques subies par leur entreprise

---

Un responsable informatique sur trois et un salarié sur cinq tiendrait pour responsable son dirigeant en cas de fuite importante de données dans lentreprise.

Tel est le constat dressé par VMware qui vient de publier les résultats d'une enquête menée par le cabinet d'études de marché Vanson Bourne. Celle-ci pertmet aussi d'établir que plus d'un tiers des entreprises s'attendent à subir une cyberattaque importante dans les trois prochains mois, qu'un quart des responsables informatiques français n'informent pas ses dirigeants en cas de cyberattaque et que seulement 11 % des dirigeants français considèrent la cybersécurité comme une priorité au détriment d'initiatives visant à revoir la sécurité de leur système d'information.
Près d'un tiers (29 %) des responsables informatiques et près d'un cinquième (21 %) des employés en France considèrent donc que leur dirigeant devrait être tenu responsable en cas d'importante fuite de données. Pourtant, un quart (25%) des responsables informatiques admet ne pas informer son dirigeant en cas d'incident de ce type. Ce manque de transparence prive donc les dirigeants, considérés comme principaux responsables, d'une visibilité réelle sur les risques que représentent les fuites de données pour leur entreprise.

L'ampleur de ce constat est encore plus frappante dans une autre enquête menée par l'Economist Intelligence Unit pour le compte de VMware en début d'année. Celle-ci révélait en effet que seuls 8 % des dirigeants d'entreprises dans la région EMEA (11% en France) considéraient la cybersécurité comme une priorité. Alors que les cyberattaques s'intensifient et deviennent de plus en plus préjudiciables pour les entreprises – avec à la clé le risque de perte de propriété intellectuelle, de positionnement concurrentiel, et de données clients – l'impact sur la performance et l'image de marque peut être considérable.

Une nouvelle approche de la sécurité s'impose
Les entreprises sont de plus en plus menacées par de graves cyberattaques : plus d'un tiers (37 %) des répondants dans la région EMEA (seulement 28 % en France) s'attendent à en être victimes dans les 3 prochains mois. Malheureusement, les approches de sécurité actuelles ne sont pas adaptées à un monde toujours plus tourné vers les technologies numériques. Ainsi, plus d'un responsable informatique français sur trois (35 %) estime que l'un des principaux risques pour son organisation réside dans le fait que les menaces évoluent plus vite que les systèmes de défense mis en place.
« Le fossé entre dirigeants et responsables informatiques est symptomatique. Il symbolise le défi que doivent relever les entreprises cherchant à repousser leurs limites, à se transformer, à se différencier et à se protéger de menaces en constante évolution », déclare Sylvain Cazard, directeur général de VMware France. « Aujourd'hui, les organisations les plus performantes sont celles qui sont capables de réagir rapidement et de préserver aussi bien leur image de marque que la confiance de leurs clients. Les applications et données des utilisateurs étant présentes sur un nombre d'appareils sans précédent, ces entreprises ont abandonné les approches traditionnelles de sécurité informatique incapables de protéger les entreprises numériques d'aujourd'hui. »

Les employés et les processus aussi problématiques que les technologies
L'un des principaux risques pour la sécurité d'une entreprise provient de l'intérieur. Ainsi, pour 45 % des responsables informatiques de la région EMEA (et 37 % en France), la négligence ou le manque de formation des employés en matière de cybersécurité représente le principal défi pour leur entreprise. L'enquête montre également jusqu'où les salariés sont prêts à aller pour accroître leur productivité : 15 % d'entre eux (contre 21% au niveau EMEA) utilisent leurs appareils personnels pour accéder à des données professionnelles, tandis que 14 % (17% en EMEA) sont prêts à enfreindre la politique de sécurité de leur entreprise afin de travailler plus efficacement.
« La sécurité n'est pas qu'une question de technologie. Comme le montrent les résultats de notre enquête, les décisions et les comportements des employés ont également un impact sur l'intégrité d'une entreprise » remarque Sylvain Cazard. « Malgré tout, la solution n'est pas non plus de tout verrouiller et d'instaurer une culture de la peur. Les organisations qui adoptent des approches intelligentes proposent plus de moyens et non de restrictions à leurs employés, leur permettant de s'épanouir, d'adapter les process et de transformer leur activité pour réussir.»
« Les entreprises tournées vers l'avenir sont conscientes du fait que les stratégies de sécurité réactives d'aujourd'hui ne sont plus efficaces pour protéger leurs applications et données. Adopter une approche software-defined garantissant l'omniprésence de la sécurité leur offre la flexibilité nécessaire pour réussir en tant qu'entreprises numériques », conclut Sylvain Cazard.
Source: infoDSI.com

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

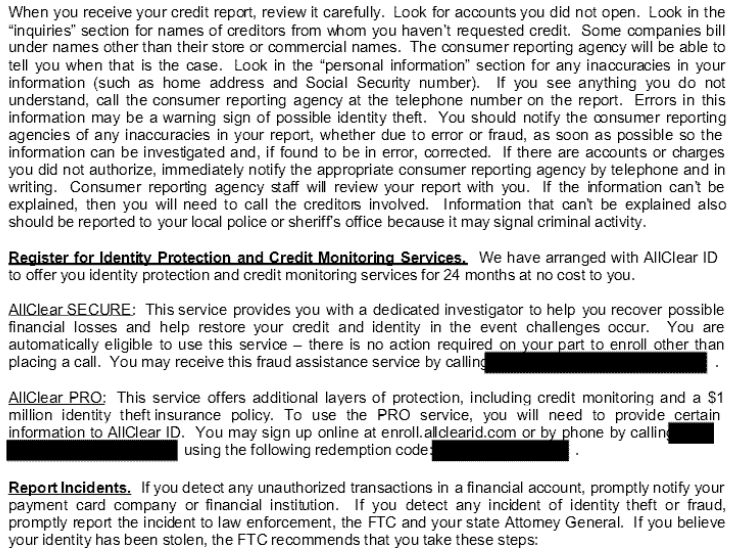
Original de l'article mis en page : Les dirigeants sont les premiers responsables en cas de cyberattaques subies par leur entreprise

---

Fuite de données chez Google

Fuite de données chez Google

Alerte pour des employés Google à la suite d'une fuite de données. Un fichier diffusé par une entreprise partenaire.



When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Register for Identity Protection and Credit Monitoring Services. We have arranged with AllClear ID to offer you identity protection and credit monitoring services for 24 months at no cost to you.

AllClear SECURE: This service provides you with a dedicated investigator to help you recover possible financial losses and help restore your credit and identity in the event challenges occur. You are automatically eligible to use this service – there is no action required on your part to enroll other than placing a call. You may receive this fraud assistance service by calling [redacted].

AllClear PRO: This service offers additional layers of protection, including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide certain information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling [redacted] using the following redemption code: [redacted].

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

Le géant de l'informatique mondial a commencé à informer, et cela depuis le mois de mai, certains de ses employés. La rumeur interne parle de plusieurs centaines. Des salariés de la firme américaine touchés par ce qui est appelé sur le sol de l'Oncle Sam « ***une violation de données*** ».

Google Data Breach pour un tiers de confiance

La fuite était indirecte, comme le précise Teri Wisness (Director of U.S. Benefits) de chez Google. La faute à l'un des fournisseurs de prestations (comptable, DRH, …) qui a envoyé un fichier électronique contenant des informations sensibles concernant des employés de Google. Sauf que le récepteur de la missive n'était pas la bonne personne. Bref, le coup classique de la pièce jointe dans un courriel. Fichier non chiffré et comportant des informations qui ne devraient pas se promener de la sorte. Je vous racontais, il y a quelques temps, le courrier de Pôle Emploi qui baladait avec lui les adresses mails des correspondants. Bref, des fuites plus nombreuses que l'on pourrait le penser… et très peu osent l'avouer.

Le géant de l'informatique a alerté toutes les autorités compétentes, comme le stipule la loi Américaine (et comme devront s'y plier les entreprise Françaises d'ici Mai 2018, NDR). Google n'a pas précisé combien d'employés ont été touchés par cette boulette !

Dans la lettre de Teri Wisness que j'ai pu lire, un guide propose des solutions et les actions mises en place pour protéger l'identité des employés impactés. A première vue, le document « perdu » comportait, en plus des identités, le numéro de sécurité sociale et d'autres données traitant d'informations bancaires.

Bref, un exemple concret d'une possibilité de fuite via un prestataire de service.

Article original de Damien BANCAL

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

=

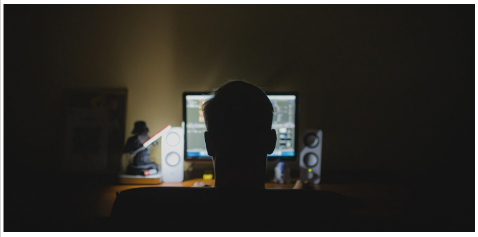
Réagissez à cet article

Original de l’article mis en page : Google Data Breach – Fuite de données chez Google – ZATAZ

Dirigeants, êtes-vous prêts à réagir en cas de cyberattaque?

Dirigeants, êtes-vous prêts à réagir en cas de cyberattaque?

Pour Nicolas Reys de la société de conseil en gestion des risques Control Risks, la question doit être soulevée en conseil d'administration.



L'ancien directeur du FBI Robert Mueller déclarait en 2014: « il y a seulement deux types d'entreprises: celles qui ont été piratés et celles qui le seront un jour. » Ce message devient de plus en plus réel. L'attaque récente sur le principal fournisseur de services de messagerie de paiements pour les institutions financières SWIFT nous rappelle que même les organisations considérées les plus sûres ne sont pas infaillibles et que maintenant les cyberattaques font désormais partie intégrante du paysage du risque des entreprises modernes. Selon une étude récente, 1.673 brèches de données ont exposé plus de 707 millions de données diverses au cours de l'année 2015, à travers le monde. Une autre étude relève que 90% des grandes entreprises et 74% des petites et moyennes entreprises dans le monde ont subi une brèche de sécurité.

Peut être très coûteux

De nombreux dirigeants considèrent toujours la réponse à une cyberattaque comme un problème purement technique et non stratégique. Pourtant la fréquence et l'ampleur croissante des cyberattaques, ainsi que l'intérêt grandissant que les partenaires commerciaux et les autorités portent à la cybersécurité, exigent d'élever le problème au rang des conseils d'administration. Certes, le lexique associé aux cyberattaques peut être intimidant pour les chefs d'entreprises, des termes tels que « centre de commandement et de contrôle », « numéro de port TCP » et « injection SQL » peuvent laisser entendre qu'une cyber intrusion est un problème informatique et donc ne concernant pas le comité de direction. Toutefois, quel qu'en soit sa nature, ce type d'événement peut être très coûteux et une réponse mal gérée est susceptible d'augmenter de manière significative son impact commercial et opérationnel. L'Institut Ponemon estime que le coût moyen d'une fuite de données est de 3,79 millions de dollars par entreprise victime; en augmentation de 23% depuis 2013.

Préjudice de réputation

A l'extrémité de ce spectre, le distributeur américain Target, qui a subi une énorme perte de données clients en 2013, estime que le coût total de cette attaque s'est élevé à 162 millions de dollars. Un montant supplémentaire de 90 millions ayant par ailleurs été couvert par les assureurs du détaillant. Mais surtout, la marque a subi un préjudice de réputation considérable et Target a vu son rythme de croissance ralentir suite à cette crise. Il est donc possible que l'impact total sur l'entreprise sera encore plus significatif à moyen terme. D'ailleurs le PDG et le responsable de la sécurité des systèmes d'information (RSSI) de Target ont été licenciés à la suite de cet événement. Bien que comprendre les dimensions techniques de ce type de crise reste crucial pour les résoudre, il faut absolument prendre en compte les implications opérationnelles et commerciales associées aux cyberattaques.
Les gestionnaires de crise au sein de l'entreprise doivent s'interroger sur au moins trois points : « quel est l'impact opérationnel immédiat sur l'entreprise de cette attaque et avec quelle rapidité pouvons-nous revenir en ligne? Quelle est notre responsabilité juridique? Avons-nous un plan de communication en place? ». Le département informatique d'une entreprise est normalement en mesure de répondre à l'incident technique et de fournir les informations sur les accès ouverts, ce qui a été volé et ce qu'il faudra faire pour reconnecter les systèmes. Mais les informaticiens ont rarement l'expérience ou le mandat pour répondre aux questions de gestion opérationnelle qu'une cyberattaque suscite.

Brèches souvent détectées par des tiers

D'autant que, les « cyberattaques » peuvent rapidement prendre des proportions médiatiques mal maîtrisées puisque Mandiant relève que 53% des brèches de sécurité informatique sont détectées par des tiers plutôt que par les victimes.
Comment se protéger? D'abord en comprenant les capacités et motivations des acteurs prenant pour cible votre entreprise afin de formuler un plan de gestion de crise adapté et proportionné, envisageant les scénarios de crises les plus probables ainsi que les plus dangereux pour votre entreprise. Il est ainsi souhaitable d'établir avant une cyberattaque, un plan de gestion de crise et des procédures bien documenté. Assurez-vous que la réponse à l'incident technique soit complète et s'accompagne d'un plan de gestion commerciale et opérationnelle. Vérifiez donc que tous les acteurs principaux de l'entreprise connaissent ce plan et qu'ils peuvent rapidement l'actionner. Testez son fonctionnement en vous exerçant dans des conditions réelles, et posez-vous les questions suivantes: Tout le monde peut-il être contacté? Connaissent-ils leurs rôles et responsabilités face à une telle crise? Enfin soyez prêts, à vous procurer le soutien de spécialiste en gestion de crise pour vous aider si vous ne disposez pas des capacités techniques, juridiques, de communications, ou de gestion de crises nécessaires en interne.
Les attaques cybercriminelles ont doublé entre 2014 et 2015, il n'est donc plus possible d'ignorer la menace. Même si vous êtes une entreprise bien protégée, une cyberattaque a toute les chances de vous affecter dans un futur proche. La question n'est déjà plus « quand aura lieu une attaque? », mais plutôt « êtes-vous prêts à réagir? »
Nicolas Reys de la société de conseil en gestion des risques Control Risks.

Article original de Challenges.fr

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

Original de l'article mis en page : Dirigeants, êtes-vous prêts à réagir en cas de cyberattaque?

Techniques et astuces pour la robustesse de vos mots de passe

Techniques et astuces pour la robustesse de vos mots de passe

Les experts en cybersécurité ont tendance à être quelque peu cyniques envers les utilisateurs « lambda », particulièrement lorsqu'il s'agit du choix des mots de passe. Cependant, selon certains experts en sécurité informatique au sein du CyLab, l'Institut Security & Privacy de l'Université de Carnegie Mellon, les utilisateurs ordinaires ne semblent pas être aussi stupides qu'il n'y paraît. En effet les erreurs commises peuvent être classées en 4 catégories spécifiques. Le travail de sensibilisation nécessaire ne devrait pas être une tâche insurmontable.

La méthodologie de CyLab est la suivante : montrer aux gens des mots de passe par paires, et leur demander lesquels leur semblent les plus robustes. Ensuite, établir une corrélation entre leurs réponses et l'efficacité effective de ces derniers en utilisant *les méthodes les plus actuelles pour craquer les mots de passe*. Au final, sur 75 paires, les participants en ont correctement sélectionné 59. Il s'agit de 79%, soit en pratique un « B ».
Il est vrai que l'échantillon des 165 utilisateurs du CyLab est certainement un peu plus technique que d'autres utilisateurs : ils ont été recrutés en ligne via le système du Turc Mécanique d'Amazon. De plus, CyLab ne dit pas en substance que tous les utilisateurs atteindront ce score, mais seulement que certains peuvent y arriver. Enfin, pour conclure, ces scores ne sont pas alarmants.
Les personnes sondées par CyLab savaient que des mots de passe sont robustes lorsque :
• Les majuscules sont utilisées au milieu du mot, plutôt qu'au début.
• Des chiffres et des symboles sont situés au milieu du mot plutôt qu'à la fin.
• Des séquences de chiffres aléatoires sont insérées à la place d'autres plus évidentes, telles que l'année en cours par exemple.
• Des noms sont ajoutés, différents des traditionnels prénoms et noms.
• Des noms faisant parties de la vie privée ne sont pas utilisés, tels que les prénoms de vos enfants.
• Des mots faisant référence de manière évidente au site ou au compte que vous êtes en train de protéger ne sont pas utilisés.
Bien sûr, il en reste 21% qui n'ont pas réussi à faire la distinction. Cela laisse en effet de belles opportunités **aux cybercriminels pour craquer vos mots de passe**. Quelles ont donc été les plus grosses erreurs commises ? :
1. **Les participants ont ajouté des chiffres à leurs mots de passe, en plus des lettres, en pensant les renforcer**. Dommage ! Les hackers savent bien que les internautes très souvent rajoutent à la fin des chiffres, du coup « brooklynqy » est plus sécurisé que « brooklyn16 ».
2. **Les participants ont pensé que le fait de changer tout simplement des lettres en chiffres rendrait leurs mots de passe plus robuste.** Dommage ! Les craqueurs de mots de passe « exploitent de plus en plus la tendance des utilisateurs à faire des substitutions prévisibles », ainsi « punk4life » n'est pas plus sûr que « punkforlife ».
3. **Les participants ont surestimé la sécurité procurée par les séquences présentes au niveau de leur clavier.**Dommage ! Les hackers de nos jours recherchent très rapidement les séquences des claviers telles que « qwertyuiop », tout comme d'autres patterns classiques, et pas seulement à base de mots.
4. **Les participants ont mal appréhendé la popularité de certains mots ou de certaines phrases.** Selon le CyLab, par exemple, les utilisateurs ont pensé que « ieatkale88 » et « iloveyou88 » étaient équivalent d'un point de vue sécurité. Pas vraiment : les craqueurs de mots de passe ont besoin de plus d'un milliard de tentatives en plus pour en venir à bout de « ilovekale ». Il est plus sûr de choisir un mot isolé rare plutôt qu'une phrase intégrant « iloveyou » or « ilove ». Les mots de passe utilisant le mot « love » sont incroyablement répandus …ce qui est plutôt une bonne intention si vous n'êtes pas responsable de la cybersécurité d'un site.
Qu'est ce qui pourrait aider les utilisateurs pour éviter les mauvaises stratégies de choix des mots de passe ? Selon l'auteur de l'étude :
Une méthode qui semble être très efficace pour assister les utilisateurs dans l'évaluation de leurs mot de passe, vis-à-vis des pratiques courantes, est de leur fournir des feedbacks ciblés et explicites pendant la phase de création. Les calculateurs actuels de la force d'un mot de passe indiquent simplement aux utilisateurs si un mot de passe est faible ou fort, mais ne mentionne pas les raisons.
Les futurs travaux dans ce domaine pourraient s'inspirer d'une récente étude qui montrait la possibilité pour les utilisateurs de finir automatiquement le mot de passe partiel qu'ils viennent de taper … et pourrait également se baser sur une autre étude utilisant des arguments de motivation ou encore la pression de collègues pour inciter les utilisateurs à créer des mots de passe plus robustes.
Article original de Sophos France

Réagissez à cet article

Original de l’article mis en page : Robustesse des mots de passes : techniques et astuces

---

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

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 perçu 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.

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

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 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 Moutain 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

Réagissez à cet article

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

---

La double authentification de

Google contournée par des hackers

La double authentification de Google contournée par des hackers

Alors que la double authentification semblait être la meilleure solution pour protéger les données personnelles des internautes, voilà que celle de Google a réussi à être contournée par des pirates. Autrement dit, les spécialistes de la sécurité vont encore devoir se creuser la tête pour trouver encore mieux !

La double authentification plombée par des pirates ?

Puisque la double identification implique qu'un utilisateur saisisse un mot de passe puis qu'il confirme son identité en saisissant un code préalablement reçu par SMS afin de pouvoir accéder à ses comptes, elle semblait être une solution fiable pour bien protéger les données des internautes.

Mais ça, c'était avant puisque des pirates ont réussi à contourner la double authentification de Google pour accéder aux comptes d'utilisateurs tiers.

Pour ce faire, les hackers ont mis en place une méthode plutôt astucieuse. En effet, s'ils disposent de l'adresse mail et du mot de passe, ils se font passer pour la firme de Mountain View, expliquent qu'une activité suspecte a été repérée et invitent l'utilisateur à renvoyer le code de sécurité qui leur a été envoyé.

Sans le savoir, les utilisateurs fournissent alors la clé de l'ultime protection aux pirates qui ont désormais le temps de commettre tous les actes malveillants qui désirent.

Une porte d'entrée vers les terminaux mobiles des utilisateurs ?

En s'offrant un accès aux comptes de messagerie des internautes, les pirates s'offrent une vraie porte d'entrée vers les terminaux mobiles de leurs propriétaires.

En effet, s'ils contrôlent le compte mail de leurs victimes, ils pourront facilement envoyer des mails sur Gmail incluant des pièces jointes frauduleuses qui peuvent être des applications malveillantes. Si le mail est ouvert depuis le mobile, le terminal sera alors automatiquement infecté.

Autrement dit, le hacker pourra avoir un accès complet à l'ensemble des données qu'il contient.

Incontestablement, la double authentification a donc ses limites…

Article original de Jérôme DAJOUX

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

Original de l’article mis en page : La double authentification de Google contournée par des hackers

---

Alerte nouveau ransomware : Le Javascript RAA est diffusé par spams

Alerte nouveau ransomware : Le Javascript RAA est diffusé par spams

---

Le ransomware RAA se propage à grande vitesse en Russie par le biais de campagnes de spams. Il prend la forme d'une pièce jointe en Javascript.

RAA, un ransomware entièrement écrit en Javascript

Si la plupart des logiciels malveillants qui ciblent des machines Windows est écrite en C++, voilà que RAA surprend puisque lui est intégralement écrit en Javascript, un langage destiné principalement à être interprété par les navigateurs web.

Pour les cybercriminels, le choix de ce langage n'est pas dû au hasard étant donné qu'ils tentent d'infecter les machines à distance via la diffusion de spams. Toutefois, tout utilisateur doit normalement agir avec méfiance avec les pièces jointes, d'autant plus si celles-ci sont dans un format Javascript. En effet, ce format doit inciter les utilisateurs à mettre le mail dans leur corbeille et surtout à ne pas ouvrir la pièce jointe.

Si tel est le cas, RAA peut faire des ravages puisqu'il est conçu pour chiffrer les documents disposant des extensions .doc, .xls, .rtf, .pdf, .dbf, .jpg, .dwg, .cdr, .psd, .cd, .mdb, .png, .lcd, .zip, .rar et .csv comme le révèlent nos confrères du Monde Informatique.

Autant dire donc que le téléchargement de la pièce jointe n'est pas sans conséquences.

Pas de vaccin disponible pour déchiffrer les contenus

S'il existe parfois des vaccins contre les ransomwares, RAA n'a pas encore le sien si bien qu'une fois vos fichiers chiffrés, vous n'aurez aucune autre alternative que payer la rançon si vous voulez débloquer de nouveau l'accès à vos documents.

Pour l'heure, ce rançongiciel se propage principalement en Russie puisqu'il semble que c'est depuis ce pays qu'opèrent les cybercriminels. Toutefois, il y a fort à parier que la diffusion de RAA va s'étendre dans les prochains mois et qu'une version « internationale » du rançongiciel sera développée par ces spécialistes du genre.

Article original de Fabrice Dupuis

Réagissez à cet article

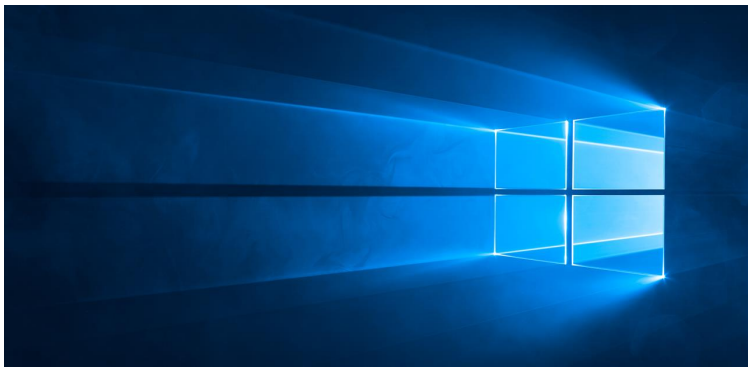
Original de l’article mis en page : RAA : un nouveau ransomware diffusé par spams

---

Microsoft corrige 44 failles de sécurité

	Microsoft corrige 44 failles de sécurité

Microsoft vient de publier une nouvelle mise à jour cumulative pour Windows 10. Elle reprend tous les correctifs de sécurité sortis depuis la dernière, mais ajoute comme d'habitude une série d'optimisations.



Patch Tuesday oblige, toute une série de bulletins de sécurité a été émise par Microsoft. 16 sont disponibles, dont 5 critiques (DNS, Office, JScript/VBScript, Edge et Internet Explorer), pour un total de 44 vulnérabilités colmatées. Toutes les versions de Windows et Office en cours de support sont touchées et il faut donc procéder à la récupération des mises à jour depuis Windows Update.

Correctifs de sécurité et réparations diverses

Dans le cas de Windows 10, cela donne lieu à une nouvelle mise à jour cumulative. Tous les correctifs de sécurité nécessaires y sont bien sûr, mais d'autres réparations sont disponibles, Microsoft restant sur son rythme d'amélioration continue de sa plateforme.

Les apports proposés sont nombreux et concernent aussi bien une meilleure fiabilité pour des composants comme Edge, Cortana, la lecture de sons, Cartes, Miracast et Explorer, que des corrections de bugs divers. Ces derniers concernaient par exemple l'affichage des bulles de notifications qui apparaissaient parfois en haut à gauche de l'écran, des solutions VPN qui ne fonctionnaient plus après certaines bascules entre cartes réseau, une position géographique qui n'était pas aussi rapidement mise à jour que nécessaire, et ainsi de suite.

Les smartphones aussi sont mis à jour

Notez que Windows 10 oblige, cette nouvelle version du système, estampillée 10586.420, se répercute également sur la mouture Mobile. Tous les smartphones l'utilisant peuvent donc se rendre dans la zone des mises à jour pour la récupérer. Il n'y a pas de liste spécifique des nouveautés, mais puisque la plupart des composants et des applications sont les mêmes que pour la mouture PC, les améliorations le sont également. On trouve mention toutefois d'un problème réglé pour lessmartphones : la sonnerie du téléphone qui s'interrompait parfois à la réception d'un SMS.

On rappellera que ces mises à jour cumulatives s'adressent pour l'instant toujours à la version 10586 mise en place initialement avec l'évolution majeure de novembre dernier, surnommée TH2, pour « Threshold 2 ». À la fin du mois prochain arrivera RS1, pour « Redstone 1 », sous la forme d'une Anniversary Update. Elle sera considérée comme le nouveau socle, déclenchant à son tour une nouvelle série de mises à jour cumulatives mensuelles.

Pour l'heure, tous les appareils disposant au minimum de Vista devraient être mis à jour sans attendre.

Article original de Vincent Hermann

Réagissez à cet article

Original de l'article mis en page : Microsoft : 44 failles colmatées et mise à jour cumulative pour Windows 10 — Next INpact