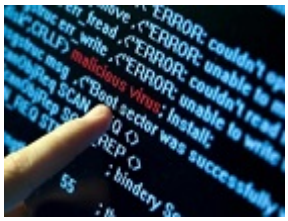
Vol de données Twitter, LinkedIn… qui est à l’origine ?



Vol de données Twitter, LinkedIn… qui est à l’origine ?

Les annonces fracassantes de vols de mots de passe se sont multipliées ces derniers temps. Attribuées dans un premier temps à un cybercriminel connu sous le nom de Peace of Mind, un second cybercriminel connu sous le nom de tessa88 clame aujourd'hui être la source originale des bases de données.

Les fuites de mot de passe se sont multipliées ces dernières semaines : Tumblr, LinkedIn, Myspace ou encore le réseau social russe Vkontakte, autant de services web qui ont vu les identifiants de leurs utilisateurs vendus à bas prix sur le web. Ces différentes fuites de données présentaient néanmoins plusieurs points communs : les données vendues étaient toutes plus ou moins datées, les entreprises concernaient ne confirmaient pas systématiquement avoir détecté un piratage de leur côté et les données étaient vendues sur une place de marché noir par un internaute répondant au pseudo Peace of Mind.
Naturellement, ce rôle de revendeur a rapidement fait peser les soupçons sur Peace Of Mind, celui-ci ne précisant pas la provenance exacte des identifiants volés qu'il proposait à la vente.

Selon Motherboard et ZDNet.com néanmoins, l'affaire est un peu plus complexe que cela et Peace Of Mind ne pourrait être qu'un vulgaire revendeur. C'est tout du moins ce que clame l'internaute dissimulé derrière le pseudo Tessa88. Ce dernier, contacté par nos confrères, clame être à l'origine des piratages massifs d'identifiants ayant surgi ces dernières semaines. Peu de détails sont connus sur la personne qui se cache derrière ce pseudonyme, mais on sait que celui-ci est apparu sur des forums russophones spécialisés dans la cybercriminalité aux alentours du mois d'avril 2016. À cette époque, elle propose à la vente des bases de données contenant des identifiants VKontakte ou Myspace parmi d'autres services.

Recel et rivalités

Pour Motherboard, plusieurs personnes pourraient se cacher derrière le pseudonyme Tessa88. Si l'internaute utilise un prénom féminin pour parler de lui sur différents forums dédiés à la cybercriminalité, le site américain soupçonne que ce pseudonyme pourrait être un avatar manipulé par un groupe de cybercriminels. Le pseudonyme avait déjà été mentionné par le site LeakedSource, qui avait fait partie des premiers sites à confirmer l'authenticité des informations contenues dans les bases de données volées mises en vente. Ceux-ci expliquaient avoir obtenu les échantillons des bases de données grâce à l'entremise de Tessa88.
Peu de temps après, Peace Of Mind propose lui aussi des bases de données similaires sur le marché noir The Real Deal : on retrouve les mêmes sites et des bases de données de tailles comparables. Mais Tessa88 n'est pas tendre avec Peace Of Mind : celle-ci clame en effet être l'auteur des piratages ayant permis de récupérer les identifiants et dénonce le fait que Peace of mind n'est qu'un revendeur, pour qui Tessa88 ne semble pas avoir beaucoup d'estime.
Peace Of Mind n'est pourtant pas un total inconnu : c'était déjà ce pseudonyme qui revendiquait la cyberattaque ayant visé le site de la distribution Linux Mint en début d'année 2016. Peace Of Mind n'a fait aucun commentaire sur les déclarations de Tessa88 et se contente de laisser entendre que la vente d'identifiants va continuer. Tessa88 laisse également entendre qu'elle n'a pas écoulé entièrement son stock et que de nouvelles ventes sont à prévoir. Tous deux clament ainsi être en possession de bases de données contenant des identifiants de connexions Instagram, là aussi dans des volumes particulièrement importants.
De nombreuses zones d'ombres persistent malgré les déclarations concurrentes des deux cybercriminels. Ainsi, ceux-ci restent muets sur l'origine exacte des données : certaines entreprises touchées n'ont reconnu aucun piratage au sein de leurs systèmes.
Impossible de savoir également pourquoi exactement ces données ressortent aujourd'hui : Tessa88 explique à Motherboard avoir exploité ces identifiants pour ses activités pendant plusieurs années, mais avoir aujourd'hui choisi de les vendre afin de faire face à des soucis de santé. La seule chose sur laquelle les deux cybercriminels s'accordent, c'est sur le fait qu'ils entendent bien continuer à revendre ces identifiants.
Article original de Louis Adam

Réagissez à cet article

Original de l’article mis en page : Twitter, LinkedIn… qui est à l’origine des vols de données ?

QRCodes : pièges à internaute ? – ZATAZ

QRCodes : pièges à internaute ? – ZATAZ

Détection du premier cas d'email frauduleux utilisant des QRCodes. Le Flashcode, une porte d'entrée à pirate qu'il ne faut pas négliger.

On retrouve ces QRcodes, baptisés aussi Flashcode, dans les journaux, la publicité… Il est possible de naviguer vers un site internet ; mettre l'adresse d'un site en marque-page ; faire un paiement direct via son cellulaire (Europe et Asie principalement) ; ajouter une carte de visite virtuelle (vCard, MeCard) dans les contacts, ou un événement (iCalendar) dans l'agenda électronique ; déclencher un appel vers un numéro de téléphone ; envoyer un SMS ; montrer un point géographique sur Google Maps ou Bing Maps ; coder un texte libre. SnapChat, par exemple, propose un QR Code maison pour suivre un utilisateur. Bref, toutes les possibilités sont ouvertes avec un QRcode. Il suffit de présenter l'image à votre smartphone, et à l'application dédiée, pour lancer la commande proposée par le QR Code. A première vue, un pirate a eu l'idée de fusionner QR Code et hameçonnage.

Fusionner QR Code et hameçonnage

Le hameçonnage, baptisé aussi Phishing/Filoutage, est une technique qui ne devrait plus être étrangère aux internautes. Pour rappel, cette attaque informatique utilise le Social Engineering dont l'objectif est la collecte des identifiants de connexion (mail, login, mot de passe, adresse IP…). Dans l'attaque annoncée il y a quelques jours par la société Vade retro, le cybercriminel a présenté son mail comme une image usurpée à un opérateur national et proposant au destinataire un remboursement consécutif à une facture payée. Le QR Code conduisait à un site présentant une page falsifiée qui incitait la victime à renseigner son identifiant et mot de passe légitime chez l'opérateur usurpé, puis présentait un message d'erreur.

L'illustration flagrante des cyber-risques pour tous

Comme le rappel Maitre Antoine Chéron, avocat spécialisé en propriété intellectuelle et NTIC aujourd'hui, presque tout le monde a une adresse électronique personnelle ou du moins professionnelle. C'est en effet devenu un mode de communication indispensable non seulement pour travailler mais également pour consommer toutes sortes de biens et services. Destinées aux particuliers, les messageries électroniques ne sont pas toujours sécurisées. Avec l'usage en masse de l'internet, et la dématérialisation des richesses, ce sont de précieux biens tels que nos données personnelles, « l'or noir du 21ème siècle », qui sont aujourd'hui convoités par les personnes mal intentionnées.

QRCodes : carrés aux angles dangereux

Les QRcodes envahissent le web et nos vies. Déjà, dès 2012, je vous informais d'une attaque découverte dans le métro parisien. Preuve que les pirates se penchaient sur la manipulation des QRcode depuis longtemps. J'ai pu rencontrer un chercheur « underground » qui s'est penché sur le sujet. Nous l'appellerons DBTJ. Il se spécialise dans la recherche de procédés détournés pour QRcode. « ***Avec mes collègues,*** explique-t-il à ZATAZ.COM, ***nous avons testés plusieurs cas, qui, hélas, se sont avérés efficaces.*** » Dans les cas de Qrcodes malveillants que j'ai pu constater : naviguer vers un site internet et se retrouver face à un code raquetteur (Ransomware) : mettre l'adresse d'un site en marque-page (Shell) ; ajouter une carte de visite virtuelle (vCard, MeCard) dans les contacts, ou un événement (iCalendar) dans l'agenda électronique, lancer un DDoS… bilan, derrière cette possibilité se cachait un vol de données et une mise en place d'usurpation d'identité.
J'ai pu constater aussi des QR Code capable de déclencher un appel vers un numéro de téléphone ou envoyer un SMS. « Nous avons réfléchis aux méthodes d'infections les plus débiles aux plus élaborés, s'amuse mon interlocuteur. Envoyer le QRcode depuis votre téléphone ; la fonctionne SMS dans SET pourrait être intéressante et ne laissera pas de traces ; utiliser le QRcode sur de faux sites, ou encore des sites vulnérables XSS (via un iframe) ; fausses publicités ; remplacer les QRcode aperçus sur des affiches. »
Ce dernier cas a été remarqué par ZATAZ.COM. Il suffit de coller un autre Flashcode, malveillant cette fois, en lieu et place de l'original sur une affiche, dans un arrête de bus par exemple. Effet malheureusement garanti. « Dans le cadre de la démonstration, nous avons infecté exactement 1.341 personnes d'une banlieue de Saint-Denis, et cela en seulement 14 heures, souligne le témoin de ZATAZ.COM. Avec une technique de SE (Social Engineering) d'une simplicité redoutable, nous avons fait des publicités contenant notre QRcode pour un jeu mobile gratuit que nous avons ensuite imprimé en plusieurs exemplaires et diffuser dans les lieux publics (gare/train – centre-ville). » ZATAZ.COM peut confirmer qu'après le test, les « pentesteurs » du QRcode ont effacé l'intégralité des informations collectées.
Bref, voilà de quoi regarder ces petits carrés noirs et blancs d'un œil nouveau … et plus suspicieux. Pour se protéger, des logiciels comme GData QRCode permettent de palier ce type d'intrusion. A utiliser sans modération.

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 : QRCodes : pièges à internaute ? – ZATAZ

Une application mobile fait sauter la banque

Une application mobile fait sauter la banque

Un chercheur en sécurité a découvert une faille critique dans une application mobile d'une banque indienne. Il aurait pu pirater l'ensemble des fonds de la banque.

Sathya Prakash aurait pu devenir l'Arsène Lupin indien en braquant 25 milliards de dollars juste en piratant l'application mobile d'une banque indienne. Mais à défaut d'être un gentlemen cambrioleur, il est chercheur en sécurité et a découvert plusieurs failles dans cette application. Dans un blog, il explique disposer d'un compte dans un établissement bancaire du secteur public. Ce dernier a décidé depuis une dizaine d'années de prendre un virage vers les nouvelles technologies.

En 2015, cette banque a décidé de publier une application mobile pour iOS et Android. Par une journée pluvieuse, le chercheur connu sous le pseudo Boris s'est donc penchée sur la sécurité de cette application. Il l'a passée au peigne fin avec des solutions de débogage pour en connaître les dessous. Lors de ce premier tour d'analyse, il a constaté des faiblesses dans certains paramètres de sécurité standards, comme la gestion du HPKP (HTTP Public Key Pinning), un mécanisme de sécurité qui protège les sites internet de l'usurpation d'identité contre les certificats frauduleux émis par des autorités de certification compromises.

Code bâclée et MiTM à la clé

Or cette fonction n'était pas utilisée par l'application. Un risque pouvant conduire à une attaque de type MiTM (Man in the Middle ou Homme du milieu) et intercepter le trafic vers et depuis la banque même s'il était chiffré et transmis en HTTPS. Il a réussi à rétrograder le chiffrement SSL de version 3 à la version 2 plus vulnérable.

Ce n'est pas tout, l'application comporte aussi des négligences dans son architecture ou tout du moins une « *révision de code bâclée* ». C'est notamment le cas pour les sessions utilisateurs qui ne comprennent pas de limite dans la durée. Traditionnellement, quand un utilisateur est inactif, il est automatiquement déconnecté et il doit initier une nouvelle session. Pas dans ce cas où le chercheur parle de sessions« *immortelles* ». En combinant ce défaut avec une attaque de type MiTM, une personne peut être en mesure de réaliser des opérations pour le compte d'un utilisateur sans avoir besoin de s'authentifier à chaque fois.

Un siphonage en règle

Enfin cerise sur le gâteau. Sathya Prakash a découvert comment l'application administre les transactions bancaires. En se penchant sur les paramètres des requêtes web, il a fait de l'ingénierie inversée et trouvé un moyen pour envoyer de l'argent d'un compte à un autre. Tout cela sans authentification. Cela signifie qu'il aurait pu siphonner la totalité des dépôts de la banque, s'élevant en 2015 à 25 milliards de dollars.

Ayant des principes et de la morale, Sathya Prakash a envoyé un mail à la banque pour lui indiquer les faiblesses et les moyens de résoudre les problèmes. La banque a pris du temps pour répondre, mais est finalement intervenue au bout de 12 jours. Dans son blog, on sent le chercheur un peu aigri de ne pas avoir reçu de primes pour ses découvertes. « *Bug Bounty = 0 dollars, Welcome to India !* », conclut-il.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Sécurité : quand une application mobile fait sauter la banque

---

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

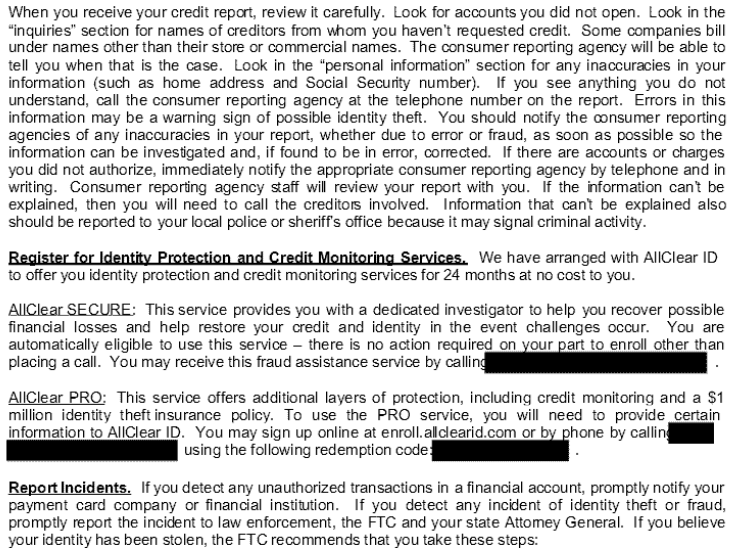
Original de l’article mis en page : La double authentification de Google contournée par des hackers

---

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

=

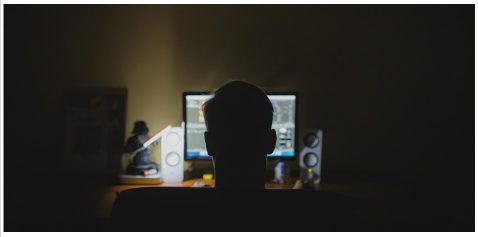
Réagissez à cet article

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