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