Image not found or type unknown

www.juventudrebelde.cu

Image not found or type unknown

Le llaman la madre de todos los hackeos, y quizá tengan razón: 3 200 millones de pares de usuarios y contraseñas relacionados con diferentes servicios de internet se han visto comprometidos y fueron filtrados hace unos días.Autor: Ilustración de Cybernews. Publicado: 17/02/2021 | 07:58 pm

La madre de todos los hackeos

Los datos de miles de millones de credenciales de cuentas relacionadas con populares servicios como Gmail, Outlook, Netflix y hasta Bitcoin se encuentran expuestos en lo que se ha llamado como la filtración de datos más grande de la historia

Publicado: Miércoles 17 febrero 2021 | 08:33:39 pm.

Publicado por: Yurisander Guevara

Le llaman la madre de todos los hackeos, y quizá tengan razón: 3 200 millones de pares de usuarios y contraseñas relacionados con diferentes servicios de internet se han visto comprometidos y fueron filtrados hace unos días.

El suceso se conoce como COMB, siglas en inglés de Compilation of Multiple Breaches. Esta compilación de múltiples hackeos fue dada a conocer por Cybernews, una publicación que se dedica a investigar temas relacionados con la seguridad de las personas en la red de redes.

De acuerdo con ese estudio, lo filtrado supondría el 40 por ciento de la población mundial (7 800 millones aproximadamente es el total), pero en términos de internet, se estima que existan unos 4 700 millones de conectados, y ello representaría el 70 por ciento, en el supuesto de que cada par de usuario-contraseña pertenezca a una sola persona.

¿Quiere saber si su contraseña se ha filtrado? Para ello Cybernews creó un servicio a partir de una base de datos que han construido con esta y otras filtraciones, la cual verifica si su correo electrónico forma parte de una

violación de seguridad. El procedimiento es sencillo: ingrese en cybernews.com/personal-data-leak-check/ e introduzca su dirección de email. Si aparece, ya tiene un motivo para preocuparse y reasegurar sus cuentas.

Un proceso en crecimiento

En Cybernews creen que la COMB no es un hackeo de un solo día. Según sus investigadores, debe estar en construcción desde 2017. Hace cuatro años se revelaba la filtración más grande —hasta ese entonces—, nombrada Breach Compilation, en la que fueron comprometidas 1 400 millones de credenciales digitales.

Lo que en ese lapso de tiempo creció sin control se reveló el martes 2 de febrero con el nombre de COMB en un foro de piratería popular. Actualmente, los datos se guardan en un contenedor cifrado y protegido con contraseña.

Los datos de COMB están organizados por orden alfabético en una estructura en forma de árbol y contienen *scripts* —código de programación— para consultar correos electrónicos y contraseñas.

Según nuestro análisis de los datos violados, hay aproximadamente 200 millones de direcciones de Gmail y 450 millones de direcciones de correo electrónico de Yahoo! en la fuga de datos de COMB, afirma Cybernews.

También está Netflix. En 2015, The Independent informó sobre un aparente «hackeo de Netflix» en el que los ciberdelincuentes pudieron iniciar sesión en las cuentas de los usuarios del servicio de video en línea bajo demanda, en todo el mundo. Sin embargo, Netflix nunca ha admitido haber sido pirateado, y es más probable que esto sea una consecuencia del hecho de que los usuarios a menudo usan las mismas contraseñas para diferentes cuentas, razona la publicación digital investigativa.

El impacto para los consumidores y las empresas con esta nueva infracción puede no tener precedentes. Debido a que la mayoría de las personas reutilizan sus contraseñas y nombres de usuario en varias cuentas, los ataques de relleno de credenciales son la mayor amenaza.

Si los usuarios utilizan las mismas contraseñas para LinkedIn o Netflix que utilizan para sus cuentas de Gmail, los atacantes pueden violar otras cuentas más importantes.

Más allá de eso, los usuarios cuyos datos se han incluido en la COMB pueden convertirse en víctimas de ataques de *spear-phishing* o recibir altos niveles de correos electrónicos no deseados.

Por qué debe preocuparle

De acuerdo con la investigación de Cybernews, en la lista de datos filtrados hay credenciales de numerosas plataformas, entre ellas Netflix, Gmail, Outlook y hasta de Bictoin.

Si bien hay servicios como Gmail que jamás han reportado una filtración de datos, muchos usuarios usan su cuenta de Google para acceder a plataformas de terceros. Por tanto, es necesario que el usuario revise a qué plataformas ha dado acceso. Más allá de cambiar la contraseña de su correo, puede revocar acceso a sitios en los que quizá se apuntó y ya no recuerda.

Para cambiar el acceso que tienen terceros a su cuenta de Google, visite la sección de Seguridad en su cuenta. En el apartado de Iniciar sesión en otros sitios web, revise las tres subsecciones que contiene para que conozca

los sitios conectados y pueda revocarlos o no.

Asimismo, es muy importante que cambie con urgencia la contraseña del correo, y trate de emplear una fuerte y difícil de averiguar. Caracteres especiales, letras en altas y bajas, además de números, siempre están entre las recomendaciones a la hora de crear una contraseña.

No es ocioso volver a recordar que a finales de 2020 un estudio de la compañía NordPass reveló que la secuencia de dígitos 123456 sigue siendo la contraseña más común empleada por los usuarios en sus diferentes servicios en internet. En segundo lugar aparecía 123456789, la cual por ser más larga no deja de ser igual de fácil de adivinar por parte de los hackers. El podio de las peores claves del año lo completó picture1.

Igual de importante es tratar de ser creativos con las contraseñas, y no usar la misma una y otra vez. Si uno de los sitios digitales que usa se ve comprometido y les roban datos —como cuando a Yahoo! le robaron más de 3 000 millones de cuentas en 2016—, sus otras redes sociales, cuentas bancarias, correos electrónicos y aplicaciones en general estarán a salvo si dedica algo de tiempo a esto.

En caso de que emplee internet regularmente, ya sea a través de conexión fija o datos móviles, active la verificación en dos pasos, o utilice un generador de contraseñas potente.

http://www.juventudrebelde.cu/suplementos/informatica/2021-02-17/la-madre-de-todos-los-hackeos