UNIVERSITY
OF
CALIFORNIA

2 de abril de 2021

A LA COMUNIDAD DE LA UNIVERSIDAD DE CALIFORNIA

Nos dirigimos a Ud. para darle una información adicional acerca de un incidente de seguridad que afecta a la comunidad de la UC y lo que Ud. debe hacer para proteger su información personal.

Como se dio a conocer el 31 de marzo, la UC es una de varias instituciones en la mira de un ciberataque a nivel nacional contra *File Transfer Appliance* (FTA) de Accellion, un servicio externo provisto para transferir información sensitiva. Este ataque ha afectado aproximadamente a 300 organizaciones, inclusive universidades, entidades gubernamentales y empresas privadas. Los autores en este incidente lograron acceder a los archivos e información personal confidencial por medio de un punto vulnerable en el programa de Accellion. Actualmente creemos que la información robada incluye, por lo menos, nombres, fechas de nacimiento, números de Seguridad Social e información sobre cuentas bancarias. Los atacantes amenazan con publicar, o de ya haber publicado, en la *web* oscura la información robada con el propósito de extorsionar organizaciones e individuos.

Estamos colaborando con entidades policiales locales y federales, y empresas que aportan servicios afines para investigar este incidente, de manera que podamos evaluar la información que haya sido comprometida, aplicar la ley y tratar de limitar la divulgación de esa información robada.

Le estamos alertando a Ud. ahora para que pueda tomar medidas de protección mientras nosotros sigamos ocupándonos de la situación.

Lo que Uds. deben hacer para proteger su información personal y financiera:

- ***Inscríbase sin costo alguno en un servicio de monitorización de crédito y protección contra robo de identidad***: Para ayudarle a proteger su identidad, le estamos ofreciendo gratuitamente a toda la comunidad de la UC una monitorización de crédito y protección contra robo de identidad, por un año, mediante Experian IdentityWorks℠. Este servicio incluye:
  - *Monitorización de crédito:* Monitoriza activamente su archivo en Experian para detectar indicios de fraude.
  - *Vigilancia de Internet:* Búsquedas tecnológicas en la *web*, salas de chat y tablillas de anuncios, 24/7, para identificar el comercio o ventas de su información personal en la *web* oscura.
  - *Restauración de identidad:* Especialistas en restauración de identidad están inmediatamente disponibles para ayudarle a Ud. a resolver problemas relacionados con fraudes crediticios o no crediticios.
  - *Experian IdentityWorks Extend CARE™:* Ud. recibirá el mismo nivel de apoyo en restauración de identidad aún después de caducar su membresía en Experian IdentityWorks.

- *$1 Millón en Seguro por Robo de Identidad:* Se proporciona cobertura por ciertos costos y transferencias electrónicas de fondos no autorizadas.
- *Pérdida de billetera:* Proporciona ayuda en las cancelaciones y reemplazos de tarjetas de crédito, débito o servicios médicos perdidas o robadas.
- *Monitorización de niños:* Hasta 10 niños de hasta 18 años de edad, vigilancia y monitorización por internet para determinar si los menores de su casa que estén inscritos tienen disponible un reporte crediticio en Experian. También se incluye restauaración de identidad y hasta $1Millón en Seguro por Robo de Identidad.

Inscríbase en el sitio web de Experian IdentityWorks usando el **código de inscripción JCZGTC333**:

- Para **adultos**, visite www.experianidworks.com/RR3Bplus
- Para **menores**, visite www.experianidworks.com/minorplus

Para ayuda con la inscripción, Ud. puede llamar al (866) 617-1923 en referencia al **número de enlace DB26512**.

- ***Monitorice y ponga alertas en su cuenta o cuentas de banco***: Monitorice su cuenta o cuentas de banco en pos de transacciones sospechosas y repórtelas a su banco. Pida a su banco monitorización y alertas *online* de su cuenta. Esto le dará a Ud. una advertencia temprana de cualquier transacción fraudulenta.

- ***Mucho ojo con los e-mails sospechosos****:* Creemos que el autor o autores del ataque a Accellion FTA pudiera(n) enviar e-mails amenazantes en cantidades masivas a fin de asustar a la gente para que les paguen dinero. Cualquiera que reciba uno de estos e-mails deberá remitirlos a la oficina de seguridad informática o sencillamente borrarlos. Por favor no les responda ni entable comunicación con ellos.

- ***Ponga un alerta de fraude en su archivo de crédito****:* Le recomendamos a Ud. que ponga un alerta de fraude en su archivo de crédito contactando a uno de los tres burós de crédito nacionales abajo listados. Si se pone un alerta de fraude en el archivo de crédito de un consumidor, luego tendrá que proceder a dar varios pasos de verificación antes de que se le extienda un nuevo crédito.
  - https://www.equifax.com/personal/
  - https://www.transunion.com
  - https://www.experian.com/

- ***Recordatorios importantes acerca de cómo protegerse a sí mismo****:* Estos incidentes nos recuerdan la importancia de hacer todo lo posible para proteger su información *online*. He aquí cinco reglas para proteger su información. Además de eso, Ud. tal vez quiera aplicar las medidas adicionales contra el robo de identidad descritas en https://www.identitytheft.gov/databreach

Para nosotros la privacidad de todos los miembros de nuestra comunidad merece nuestra mayor seriedad. Mantendremos a la comunidad de la UC al corriente a medida que tengamos más información y podramos compartirla.