Aviso Sustituible de Violación de Datos

Este es un anuncio sobre un ataque de phishing contra el Condado de Los Ángeles, Departamento de Salud Pública ("DPH") que puede afectar la privacidad de cierta información personalmente identificable y/o de salud de algunos clientes del DPH, empleados y otras personas. El DPH toma este incidente en serio y ha cooperado con las autoridades en este asunto.

¿Qué sucedió?

Entre el 19 de febrero de 2024 y el 20 de febrero de 2024, el DPH sufrió un ataque de phishing. Específicamente, un actor de amenazas externas pudo obtener los datos de inicio de sesión de 53 empleados del DPH a través de un correo electrónico de phishing. Un correo electrónico de phishing es un correo electrónico fraudulento que parece provenir de una fuente legítima con el objetivo de engañar al destinatario para que divulgue datos sensibles. En este caso, los empleados del DPH hicieron clic en el enlace ubicado en el cuerpo del correo electrónico, pensando que estaban accediendo a un mensaje legítimo de un remitente confiable.

Debido a una investigación de las autoridades, se nos aconsejó retrasar la notificación de este incidente, ya que la divulgación pública podría haber obstaculizado su investigación.

¿Qué información estuvo involucrada?

La información identificada en las cuentas de correo electrónico potencialmente comprometidas podría haber incluido el nombre y apellido de los clientes del DPH/empleados/otras personas, fecha de nacimiento, diagnóstico, recetas, número de expediente médico/ID del paciente, número de Medicare/Med-Cal, información del seguro médico, número de Seguro Social y otra información financiera.

Las personas afectadas pueden haber sido impactadas de manera diferente y no todos los elementos mencionados aplicaron para cada persona.

Lo que estamos haciendo

El DPH ha implementado varias mejoras para reducir nuestra exposición a ataques de correo electrónico similares en el futuro. Tras descubrir el ataque de phishing, actuamos rápidamente para desactivar las cuentas de correo electrónico afectadas, restablecer y volver a cargar los dispositivos del usuario, bloquear los sitios web identificados como parte de la campaña de phishing y poner en cuarentena todos los correos electrónicos entrantes sospechosos. Además, se distribuyeron notificaciones de concienciación a todos los miembros del personal del DPH para recordarles que estén atentos al revisar correos electrónicos, especialmente aquellos que incluyan enlaces o archivos adjuntos. Se notificó a las autoridades al descubrir el ataque de phishing, y las mismas investigaron el incidente.

Además de notificar a las personas potencialmente afectadas por este incidente, notificaremos al Departamento de Salud y Servicios Humanos de EE. UU., Oficina de Derechos Civiles y a otras agencias según lo requiera la ley y/o el contrato.

Estamos buscando mantenernos al tanto de las amenazas a los sistemas de macrodatos que están en constante evolución. El DPH sigue vigilante en sus esfuerzos por proteger la información confidencial y continúa fortaleciendo su programa de privacidad y seguridad de la información para implementar salvaguardias que prevengan y/o reduzcan los ciberataques.

Lo que puede hacer usted

Aunque el DPH no puede confirmar si se accedió a la información o se utilizó de manera indebida, alentamos a los clientes/empleados/otras personas, a revisar el contenido y la precisión de la información en su expediente médico con su proveedor médico.

Para ayudar a aliviar las preocupaciones y restaurar la confianza después de este incidente, hemos contratado los servicios de Kroll, un líder global en mitigación de riesgos y respuesta, para proporcionar monitoreo de identidad durante un año sin costo para los clientes afectados.

Además, los clientes afectados deben revisar los "Pasos que puede tomar para protegerse contra el robo de identidad y el fraude", para ayudar a proteger su información.

Para obtener más información

Los clientes del DPH y empleados que deseen consultar si su información se vio afectada pueden comunicarse con el centro de llamadas dedicado y establecido disponible sin costo en los EE. UU. al 1-866-898-4312, de 6:00 a. m. a 5:00 p. m. Hora del Pacífico (excluyendo fines de semana y días festivos importantes en EE. UU.).

PASOS QUE PUEDE TOMAR PARA PROTEGERSE CONTRA EL ROBO DE IDENTIDAD Y EL FRAUDE

Revisar y monitorear su información médica, explicación de beneficios

Le animamos a revisar su expediente médico con su proveedor médico para asegurarse de que el contenido sea correcto y preciso. También puede revisar la(s) declaración(es) de Explicación de Beneficios que reciba de su proveedor de atención médica o plan de salud. Si ve algún servicio que cree que no recibió, comuníquese con su proveedor de atención médica o plan de salud al número de teléfono que aparece en la declaración de Explicación de Beneficios, o comuníquese con su proveedor de atención médica o plan de salud y pida que le envíen una copia de su declaración después de cada consulta.

Solicitar informes de crédito

El condado le anima a mantenerse al pendiente contra incidentes de robo de identidad y fraude, revisar sus estados financieros y monitorear sus informes de crédito en busca de actividad sospechosa. Según la ley de Estados Unidos, usted tiene derecho a un informe de crédito gratuito al año de cada una de las tres principales agencias de informes crediticios. Para solicitar su informe de crédito gratuito, visite www.annualcreditreport.com o llame gratis al 1-877-322-8228. También puede ponerse en contacto directamente con las tres principales agencias de crédito que se mencionan a continuación para solicitar una copia gratuita de su informe de crédito:

Equifax **P.O. Box 740241** **Atlanta, GA 30374** **(800) 525-6285** **www.Equifax.com**	**Experian** **P.O. Box 9532** **Allen, TX 75013** **(888) 397-3742** **www.Experian.com**	**TransUnion** **P.O. Box 1000** **Chester, PA 19022** **800-916-8800** **www.transunion.com**

Las agencias de crédito pedirán un Número de Seguro Social (SSN, por sus siglas en inglés) y otra información personal para fines de identificación. Una vez que se ponga en contacto con una agencia de crédito, recibirá una carta con instrucciones sobre cómo obtener sus informes de crédito gratuitos. Revise los informes para asegurarse de que su información personal, como la dirección y el SSN, sea precisa. Si hay algo que no entienda, llame a la agencia de informes de crédito al número de teléfono que aparece en el informe y pida una explicación.

Si descubre que su información ha sido utilizada de manera incorrecta, o que se ha creado una cuenta falsa utilizando su identidad, contacte al departamento de policía local, a su banco y a sus agencias de tarjetas de crédito. Debe obtener una copia del informe policial en caso de que necesite dar copias del mismo a los acreedores para aclarar los registros. Aunque no encuentre indicaciones de fraude en los informes, debe revisar su informe de crédito cada tres meses durante el próximo año y llamar a los números de las agencias de crédito mencionados arriba para solicitar informes y mantener la alerta de fraude (descrita a continuación) activa.

Solicitar alertas de fraude

Usted, o su representante legal, también puede solicitar a estas agencias de crédito que coloquen una Alerta de Fraude en su expediente, la cual alertará a los acreedores para que tomen medidas adicionales para verificar su identidad antes de otorgar crédito a su nombre. Tenga en cuenta que, debido a que una Alerta de Fraude indica a los acreedores que sigan ciertos procedimientos para protegerlo, también puede retrasar su capacidad para obtener crédito mientras la agencia verifica su identidad. En cuanto una agencia de crédito confirme su Alerta de Fraude, las demás son notificadas para colocar Alertas de Fraude en su expediente. Si desea colocar una Alerta de Fraude, o si tiene alguna pregunta sobre su informe de crédito, por favor póngase en contacto con cualquiera de las agencias mencionadas anteriormente.

Solicitar un congelamiento de seguridad

También puede colocar un congelamiento de seguridad en sus informes de crédito. Un congelamiento de seguridad prohíbe a una agencia de crédito divulgar cualquier información de su informe de crédito sin su autorización por escrito. Sin embargo, tenga en cuenta que colocar un congelamiento de seguridad en su informe de crédito puede retrasar, interferir o prevenir la aprobación oportuna de cualquier solicitud que realice para nuevos préstamos, hipotecas, créditos, empleo, vivienda u otros servicios. Necesitará colocar un congelamiento de seguridad por separado con cada una de las tres principales agencias de crédito enumeradas a continuación si lo desea en todos sus expedientes de crédito. Una agencia de crédito no tiene permitido cobrarle por colocar, levantar o quitar un congelamiento de seguridad si has sido víctima de robo de identidad y proporciona a la agencia de crédito un informe policial válido. En todos los demás casos, cada agencia de crédito puede cobrarle una tarifa para colocar, levantar temporalmente o eliminar permanentemente un congelamiento de seguridad. Para obtener más información sobre cómo colocar un congelamiento de

seguridad, puede utilizar la siguiente información de contacto:

Congelamiento de seguridad de Equifax
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com/personal/credit-report-services/credit-freeze/

Congelamiento de seguridad de Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

Congelamiento de seguridad de TransUnion
P.O. Box 160
Woodlyn, PA 19094
800-916-8800
www.transunion.com/credit-freeze

Información Adicional

Puede obtener más información sobre robo de identidad, alertas de fraude y los pasos que puede tomar para protegerse, contactando a la Comisión Federal de Comercio (FTC, por sus siglas en inglés) o al Fiscal General de su estado. La Comisión Federal de Comercio también anima a aquellos que descubran que su información ha sido mal utilizada a presentar una queja con ellos. Puede contactar a la Comisión Federal de Comercio en: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.identitytheft.gov ; 1-877-ID-THEFT (1-877-438-4338); y TTY: 1-866-653-4261.

También puede ponerse en contacto con la FTC con los datos anteriores si necesita más detalles sobre cómo presentar una queja con ellos. **Los casos conocidos o sospechosos de robo de identidad también deben ser reportados a las autoridades locales y al Fiscal General de su estado.**

Visite la Oficina de Protección de la Privacidad de California para obtener información adicional sobre la protección contra el robo de identidad: https://oag.ca.gov/privacy