AVISO SUSTITUTORIO DE VIOLACIÓN DE DATOS

De conformidad con las leyes federales y estatales, esto proporciona un aviso sustitutorio

Este es un anuncio sobre un ataque de phishing contra el Departamento de Servicios de Salud ("DHS") del Condado de Los Ángeles que puede afectar la privacidad de parte de información de identificación personal y/o de salud de ciertos pacientes de DHS. El DHS está tomando este incidente en serio y estamos trabajando y cooperando con las fuerzas del orden en este asunto.

¿Qué ocurrió?

Durante los días 19 de febrero, 2024, y 20 de febrero 2024, el DHS sufrió un ataque de phishing. Específicamente, un pirata informático pudo obtener las credenciales de inicio de sesión de 23 empleados del DHS a través de un correo electrónico de phishing. Un correo electrónico de phishing intenta engañar a los destinatarios para que entreguen información importante. En este caso, los empleados del DHS hicieron clic en el enlace ubicado en el contenido del correo electrónico, pensando que estaban accediendo a un mensaje legítimo de un remitente confiable.

Debido a la investigación en curso por parte de las fuerzas del orden, se nos aconsejó que retrasáramos la notificación de este incidente hasta hoy, ya que el aviso público pudo haber obstaculizado su investigación.

¿Qué información estuvo involucrada?

La información identificada en las cuentas de correo electrónico potencialmente comprometidas puede haber incluido nombre y apellido, fecha de nacimiento, domicilio, número(s) de teléfono, dirección de correo electrónico, número de registro médico, número de identificación de cliente, fechas de servicio y/o información médica (por ejemplo, diagnóstico/afección, tratamiento, resultados de pruebas, medicamentos) y/o información de su plan de salud. La información no incluía números de Seguro Social (SSN, por sus siglas en inglés) ni información financiera.

Es posible que las personas afectadas se hayan visto afectadas de manera diferente y no todos los elementos enumerados estaban presentes para cada individuo.

Lo que estamos haciendo

El DHS ha implementado numerosas mejoras para reducir nuestra exposición a ataques similares por correo electrónico en el futuro. Al descubrir el ataque de phishing, actuamos rápidamente para desactivar las cuentas de correo electrónico afectadas, restablecer y volver a crear imágenes de los dispositivos del usuario, bloqueamos los sitios web identificados como parte de la campaña de phishing y pusimos en cuarentena todos los correos electrónicos entrantes sospechosos. Además, se distribuyeron notificaciones para crear conciencia en todos los miembros de la fuerza laboral del DHS para recordarles que estén atentos al revisar los correos electrónicos, especialmente aquellos que incluyen enlaces o archivos adjuntos. Las fuerzas del orden fueron notificadas al descubrir el ataque de phishing e investigaron el incidente.

También iniciamos una revisión administrativa e implementamos controles adicionales para minimizar el riesgo de futuros ataques de phishing contra las cuentas de correo electrónico del DHS. Además, mejoramos la capacitación para identificar y responder a los ataques de phishing como parte del programa continuo para crear conciencia sobre la seguridad cibernética del DHS.

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

Buscamos mantenernos a la vanguardia de las amenazas continuas y su rápida evolución en los grandes sistemas de datos. El DHS permanece vigilante en sus esfuerzos por proteger la información confidencial y continúa fortaleciendo su programa de privacidad y seguridad de la información para implementar salvaguardas para prevenir y/o reducir los ataques cibernéticos.

Lo que usted puede hacer

Si bien el DHS no puede confirmar que se haya accedido a su información o que esta se haya utilizado indebidamente, alentamos a los pacientes a revisar el contenido y la exactitud de la información en su registro médico con su proveedor médico. Aunque la información potencialmente comprometida no contenía números de seguro social ni información financiera, las personas afectadas pueden revisar los "Pasos que puede tomar para protegerse contra el robo de identidad y el fraude" publicados en https://dhs.lacounty.gov.

Para mayor información

Entendemos que puede haber preguntas adicionales sobre este incidente y hemos establecido un centro de llamadas exclusivo disponible de forma gratuita en los EE. UU. Llame al 1 (866) 528-2114, de 6:00 a. m. a 5:00 p. m., horario del Pacífico (excluyendo fines de semana y los principales días festivos de los EE. UU.). Las personas afectadas también pueden visitar el siguiente sitio web para obtener más información: https://dhs.lacounty.gov.