Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

BANCO SANTANDER SUFRE ATAQUE CIBERNÉTICO MASIVO

14 / 05 / 2024

CONTENIDO

INTRODUCCIÓN

En el panorama actual de amenazas cibernéticas cada vez más sofisticadas, la seguridad de la información se ha convertido en una preocupación central tanto para empresas como para individuos. Los recientes incidentes, como el ciberataque al Banco Santander, resaltan la importancia de adoptar medidas proactivas para proteger los datos sensibles contra posibles intrusiones. En este contexto, es crucial implementar prácticas de ciberseguridad robustas y estar al tanto de las últimas recomendaciones para mitigar riesgos y salvaguardar la integridad de la información.

BANCO SANTANDER SUFRE ATAQUE CIBERNÉTICO MASIVO

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_05_14_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	14/05/2024
Es día cero (0 day):	No

RESUMEN

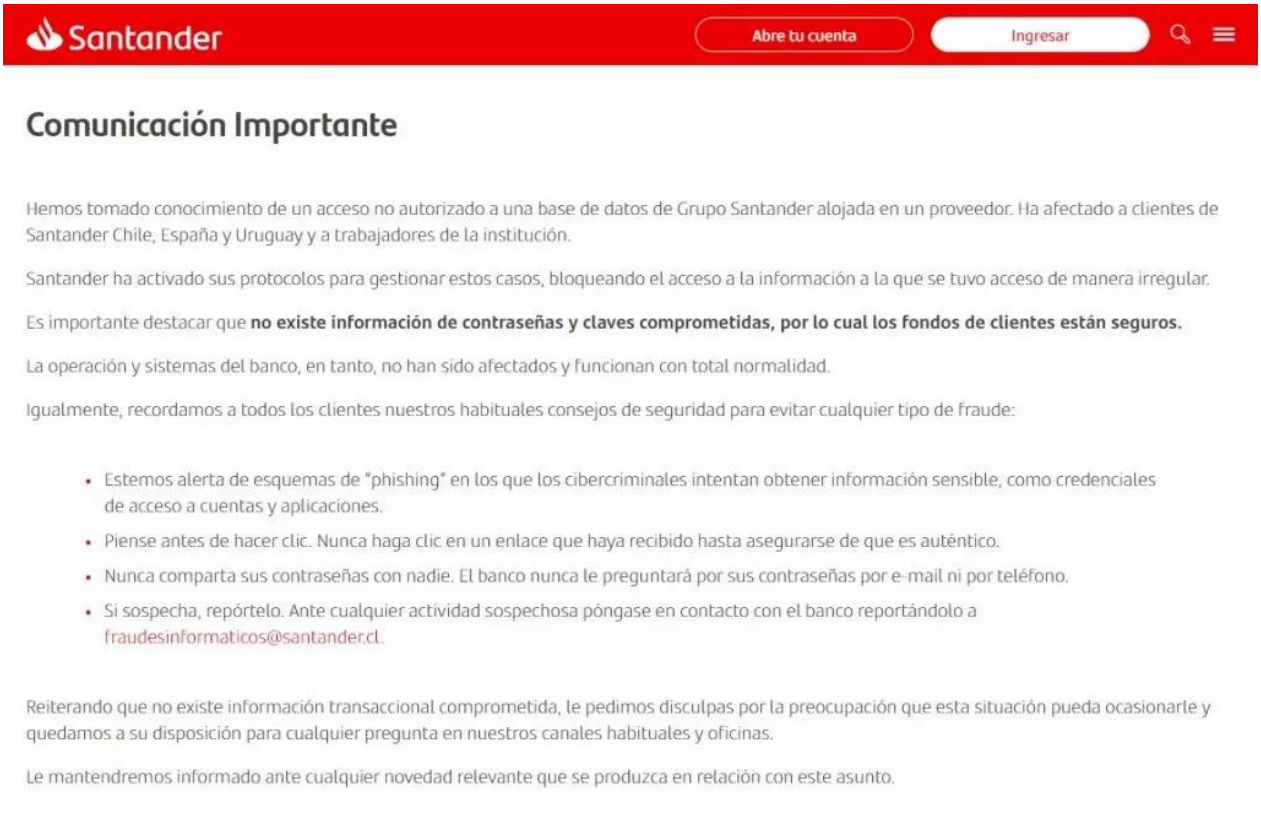
En un comunicado emitido hoy, el Banco Santander ha confirmado ser víctima de un ciberataque a gran escala, comprometiendo la seguridad de datos de clientes en España, Chile y Uruguay. El incidente, que ha sacudido la confianza en la seguridad bancaria, ha expuesto información sensible de clientes, así como detalles de empleados actuales y anteriores.

Naturaleza del Ataque y Alcance

El ataque, dirigido a una base de datos alojada por un proveedor del banco, ha permitido un acceso no autorizado a información confidencial. Aunque el banco asegura que no se han visto comprometidas credenciales de acceso o contraseñas para operar en línea, el acceso a datos personales sigue siendo una preocupación seria para los afectados.

Respuesta del Banco Santander

En respuesta a este incidente, el Banco Santander ha tomado medidas inmediatas para mitigar el impacto y garantizar la seguridad de sus sistemas. Además de informar proactivamente a los clientes y empleados afectados, el banco ha colaborado estrechamente con las autoridades y reguladores pertinentes para abordar este ataque cibernético.



Santander

Abre tu cuenta

Ingresar

Comunicación Importante

Hemos tomado conocimiento de un acceso no autorizado a una base de datos de Grupo Santander alojada en un proveedor. Ha afectado a clientes de Santander Chile, España y Uruguay y a trabajadores de la institución.

Santander ha activado sus protocolos para gestionar estos casos, bloqueando el acceso a la información a la que se tuvo acceso de manera irregular.

Es importante destacar que **no existe información de contraseñas y claves comprometidas, por lo cual los fondos de clientes están seguros.**

La operación y sistemas del banco, en tanto, no han sido afectados y funcionan con total normalidad.

Igualmente, recordamos a todos los clientes nuestros habituales consejos de seguridad para evitar cualquier tipo de fraude:

- Estemos alerta de esquemas de "phishing" en los que los cibercriminales intentan obtener información sensible, como credenciales de acceso a cuentas y aplicaciones.
- Piense antes de hacer clic. Nunca haga clic en un enlace que haya recibido hasta asegurarse de que es auténtico.
- Nunca comparta sus contraseñas con nadie. El banco nunca le preguntará por sus contraseñas por e-mail ni por teléfono.
- Si sospecha, repórtelo. Ante cualquier actividad sospechosa póngase en contacto con el banco reportándolo a fraudesinformaticos@santander.cl.

Reiterando que no existe información transaccional comprometida, le pedimos disculpas por la preocupación que esta situación pueda ocasionarle y quedamos a su disposición para cualquier pregunta en nuestros canales habituales y oficinas.

Le mantendremos informado ante cualquier novedad relevante que se produzca en relación con este asunto.

Recomendaciones de Seguridad

- Para protegerse de posibles intentos de fraude relacionados con este incidente, el Banco Santander ha emitido una serie de recomendaciones clave:
- Verificar la Identidad: Nunca proporcionar información confidencial, como códigos o claves bancarias, a personas que afirmen ser empleados del banco por teléfono o correo electrónico.
- Contactar por Canales Oficiales: Ante cualquier duda, siempre es mejor contactar con el banco a través de los canales oficiales para confirmar la autenticidad de cualquier comunicación recibida.
- Reportar Actividad Sospechosa: Se ha habilitado un correo electrónico específico (reportphishing@gruposantander.com) para informar sobre cualquier mensaje sospechoso de ser una estafa.
- Contáctenos para conocer más sobre nuestro servicio de “valoración de proveedores”, para así, tomar las medidas necesarias.

Evitar Enlaces Sospechosos: Nunca acceder a la banca en línea a través de enlaces recibidos por correo electrónico no solicitado, y no responder a notificaciones de seguridad relacionadas con cuentas bancarias si no se han solicitado.

Conclusión

Este ataque al Banco Santander sirve como un recordatorio urgente de la importancia de la seguridad cibernética en el sector financiero. Las empresas deben permanecer vigilantes y adoptar medidas proactivas para proteger la información sensible de sus clientes y empleados. En un mundo digital cada vez más interconectado, la seguridad cibernética se convierte en una prioridad ineludible para garantizar la confianza y la integridad de las operaciones bancarias en línea

NOTICIA COMPLETA

https://devel.group/blog/banco-santander-sufre-ataque-cibernetico-masivo/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente