BCR -MAZE

DC11506 - HACKING COSTA RICA.

ACERCA DE.

A día de hoy, una de las noticias que mayor movimiento ha generado en medios, es la relacionada a la **exfiltración anunciada por la SUGEF**, señalando la obtención de datos pertenecientes al Banco de Costa Rica por terceros, tales como transacciones, cuentas bancarias, etc...

El cuándo y el cómo siguen siendo un misterio, ante una creciente de la especulación, señalando un impacto menor debido a que dicha información **NO es actual** y **NO existen indicios de intrusión**, según fuentes oficiales.

Como parte de la responsabilidad social, ética y profesional por parte de los miembros que forman **La Comunidad de Seguridad DC11506**, compartimos ante ustedes, algunas ideas asociadas al "¿Que hacer?", "¿Que no hacer?"; ante una situación como la expuesta anteriormente, el correcto manejo de esta situación permite **no exponer de forma participativa nuestra información** y la de todos.

STAFF
DC11506

contact@dc506.org

¿QUÉ HACER?

Monitorear sus estados de cuenta, transacciones y cualquier movimiento anómalo, así asegurando una mejor visibilidad ante transacciones fraudulentas. **Esto debería ser una práctica a realizar frecuentemente.**

Gran parte de las instituciones financieras permiten configurar alertas en caso de transacciones sospechosas. Con respecto a este caso en particular, a pesar de que el banco manifestó que la mayoría de la información liberada no es actual si usted tiene dudas, **contacte al banco a través de sus canales oficiales o acérquese a una sucursal**.

Basado en las declaraciones del gerente del BCR, el **Banco de Costa Rica estará haciendo reposiciones del plástico sin costo para las personas que así lo deseen.**

¿QUÉ NO HACER?

A consecuencia de la exfiltración de datos, la exposición de los mismos ha generado la **creación de sitios de consulta**, verificando así si su número de cuenta fue parte de esta exfiltración. **La recomendación tanto del Banco de Costa Rica como de la Comunidad es NO hacer uso de estos servicios de terceros.**

Se desconoce el uso que se le puedan dar a sus datos una vez ingresados. A pesar de que algunos de estos sitios cuentan con “políticas de uso de datos" **no se debe confiar de éstas ya que éstos sitios no están asociados ante ningún ente regulador o emisor de tarjetas.**

Sitios de este tipo pueden ser utilizados para **distribuir software malicioso**.

Este tipo de sitios no oficiales pueden dar cabida para que personas con fines maliciosos hagan copias de los mismos (Phishing Sites), y los distribuyan entre usuarios finales. **Estos sitios de “Phishing” podrían recolectar datos de los usuarios finales y hacer uso de ellos con fines maliciosos**.

Para más información acerca de Phishing puede referirse a la misma información distribuida por BCR.

Finalmente la mayoría de estos sitios de verificación pueden haber sido elaborados en cuestión de horas, por lo que **no garantizan que hayan sido desarrollados con las mejores prácticas y estándares en materia de seguridad**. Por esta misma razón varios de estos sitios son reportados en este momento como sitios maliciosos por varios Antivirus y motores de búsqueda.

STAFF
DC11506

contact@dc506.org

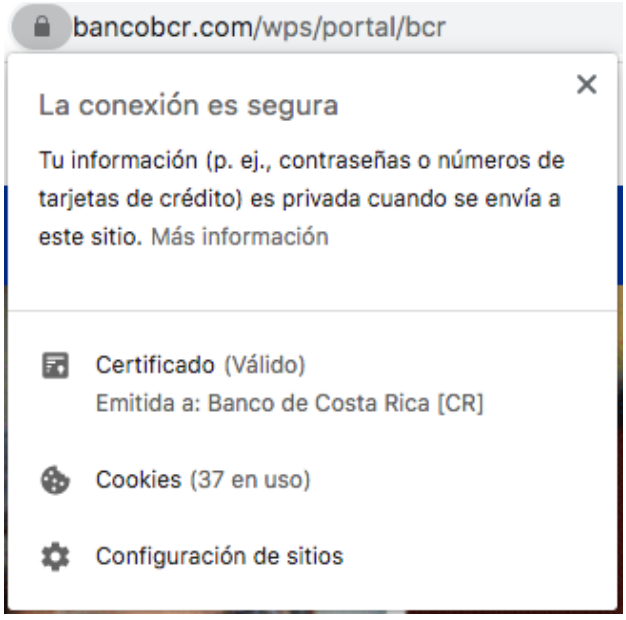
RECOMENDACIONES GENERALES.

La base de datos filtrada por los cibercriminales ha sido publicada en varios sitios, incluyendo el popular sitio Github.

La recomendación en este caso de nuevo es **NO descargar ningún archivo de estos sitios a menos de tener un amplio conocimiento en manejo y análisis de malware.**

En muchos casos estos archivos pueden contener software malicioso, que podrían terminar dañando y/o accediendo a la información confidencial en su computadora.

Verifique en todo momento la dirección del sitio.



Verificar que la conexión sea segura, es el primer paso.

- En caso de tener dudas **asesórese a través de los canales oficiales del banco**.

- Solicite una reposición de su plástico en caso de que **lo considere necesario**.

- Haciendo uso de la banca en línea **evite la reutilización de contraseñas**, asegúrese de que la contraseña de sus sitios bancarios sea **única y difícil de adivinar.**

  Hay múltiples tutoriales en internet y password managers como 1Password para generar y salvaguardar ésta información.

- Únicamente acceda a páginas de banca desde equipos que sean de su **entera confianza**, deseablemente que tenga un antivirus instalado, así como su Sistema Operativo en su última versión.

- **Confirme que la conexión al sitio web sea válida y encriptada**. Ésto va a asegurar que su conexión sea segura y sus datos no puedan ser capturados ni manipulados.

- La mayoría de las instituciones bancarias cuenta con **un segundo factor de autenticación**, para el ingreso en línea sea a través de un token, aplicación generadora de códigos, clave dinámica o de la forma que el banco lo sugiera. **Solicite el suyo**.

- No brindé información confidencial respecto a números de cuenta o tarjetas a través de teléfono, email o sitios web no autorizados. **El banco nunca va a pedir su clave o clave dinámica por ninguna vía de comunicación electrónica.**

STAFF
DC11506

contact@dc506.org

BCR -MAZE

DC11506 - HACKING COSTA RICA.

RECORDEMOS QUE LA SEGURIDAD ES RESPONSABILIDAD DE TODOS!

STAFF
DC11506

contact@dc506.org

DC11506 - DEF CON GROUP.
COMUNIDAD DE HACKERS Y EXPERTOS EN SEGURIDAD INFORMÁTICA DE COSTA RICA.