ATON

El asesor presidencial de ciberseguridad, Jorge Atton.

Autoridades presentan denuncia por "alarma pública"

Desde el 25 de julio que las filtraciones de datos personales no han cesado, afectando principalmente a la industria bancaria.

De hecho, la Superintendencia de Bancos e Instituciones Financieras ya presentó una denuncia ante el Ministerio Público el 27 de julio, por el incidente que afectó a más de 14 mil tarjetas de crédito.

Sin embargo, las autoridades continúan investigando la naturaleza de los acontecimientos.

El asesor presidencial de ciberseguridad, Jorge Atton, se reunió ayer con el superintendente de Bancos, Mario Farren, y anunciaron que interpondrán una nueva denuncia ante la fiscalía. "Vamos a presentar, como Ministerio del Interior, una denuncia por alarma pública, y eso va a ser materia de investigación", dijo Atton.

El regulador señaló que la información que se ha dado a conocer no está sujeta a reserva, por lo que no sería información filtrada por alguna institución, lo que finalmente buscaría generar molestias.

Cómo prevenir que se fugue la información

Las múltiples filtraciones de datos dejan en alerta a los usuarios ante posibles fraudes o mal uso de su información.

El socio de ciberseguridad de Deloitte, Nicolás Corrado, sostiene que lo primero y más importante para resguardar la propia seguridad y protegerse de ataques es tomar conciencia de dónde se publica la información.

El experto menciona que las medidas preventivas son variadas y entre ellas se cuentan:

- Ser conscientes de los datos que se solicitan, para qué los piden y si es atinente la solicitud.
- Evitar dar información de más.
- No realizar compras o introducir datos críticos en computadores que no sean propios.
- No comprar en sitios que no sean reconocidos y realizar las compras en canales web encriptados. Tampoco comprar a través de redes sociales.
- Saber que el CVV (código de 4 o 3 dígitos de las tarjetas de crédito) es el dato más crítico para los pagos, por lo que siempre hay que corroborar dónde se incorpora.
- Evitar que aplicaciones móviles y sitios web recuerden los datos críticos o tarjetas de crédito.

Además, Corrado menciona que ya varios bancos permiten hacer compras y usar tarjetas virtuales, que son números distintos a la tarjeta física y se usan por única vez y en tiempos acotados de vencimiento, como medida de precaución.

¿Qué hacer en caso de verse afectado ?

El superintendente de Bancos e Instituciones Financieras, Mario Farren, y el socio de ciberseguridad de Deloitte, Nicolás Corrado, entregaron algunas recomendaciones para enfrentar de mejor forma una posible filtración de datos personales:

- Realizar las consultas pertinentes a través de las aplicaciones, páginas o simplemente acercarse a una sucursal del banco, en el caso de que se descubra algún movimiento sospechoso en la cuenta.
- Una vez filtrada la información, verificar que el banco haya realizado el bloqueo de tarjetas o de la información filtrada y revisar los últimos movimientos financieros.
- Ver la actividad en forma detallada durante el mes para evitar cargos que sean imputados más adelante. En caso de detectarse el uso indebido de los datos, se debe notificar al banco y seguir los procedimientos del mismo para rechazar el cargo.
- Si el banco lo permite, activar las alarmas *online* que notifican con cada uso de la tarjeta para estar alertas.
- Exigir información a los bancos y ver qué es lo que están haciendo en concreto para tener un conocimiento de las políticas respecto al manejo de fraudes.
- En caso que se detecte un uso o cargo posterior a la fecha de solicitud de bloqueo será responsabilidad del banco. El bloqueo contempla cambiar el plástico (la tarjeta) por un número nuevo.