

Ciudad de México, a 18 de julio de 2023.

ASUNTO: Síntesis del COMUNICADO: ALERTA INAI SOBRE ROBO DE DATOS DE TARJETAS DE CRÉDITO O DÉBITO.

El lunes 17 de julio de 2023, el INAI emitió el comunicado de prensa INAI/206/23.

(<https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-206-23.pdf>)

De dicho **COMUNICADO** se destaca lo siguiente:

- El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) advierte respecto a la estrategia denominada Carding, utilizada para obtener los datos de las tarjetas de crédito o débito, cuyo objetivo es obtener los datos numéricos de la tarjeta, incluido el código de verificación.
- Los delincuentes suelen utilizar diversos métodos para obtener los datos, por ejemplo, mediante llamadas telefónicas un operador convence a las personas de que le den su número de tarjeta de crédito, o a través de Internet recibiendo un correo electrónico engañoso en el que solicitan estos datos.
- Una de las técnicas más usadas para obtener los números de las tarjetas, se denomina **Shoulder surfing**: en este caso, una persona simplemente mira disimuladamente el número de la tarjeta cuando se va a pagar y lo memorizan, al igual que el código de verificación.
- En las compras en línea suelen utilizarse tiendas falsas con ofertas que realmente no existen. Una vez que se ingresan los datos, los ciberdelincuentes se quedan con el número de tarjeta y el producto jamás llega.
- Los datos de las tarjetas son utilizados para realizar compras que no suelen ser muy grandes, sino cargos recurrentes como pagos de cuentas de **Spotify, Netflix, YouTube, Uber** o suscripciones mensuales a videojuegos, de manera que los importes sean pequeños y secuenciales, para evitar levantar sospechas y que sea difícil darse cuenta de que la estafa está sucediendo.

Para prevenir el Carding, el INAI recomienda:

1. Nunca perder de vista la tarjeta cuando se utilice de manera física para realizar pagos.
2. Evitar que la persona que realice el cobro digite el Código de Verificación o CVV, es preferible solicitar la terminal para que sea el titular quien ingrese los datos.



SALAZAR & SOLÍS
ABOGADOS

3. Verificar que las páginas donde se realizarán las compras en línea cumplan con el protocolo de seguridad: deben iniciar con “https” y mostrar la figura de un candado cerrado en la barra de dirección.
4. No utilizar redes o computadoras públicas al momento de realizar compras.
5. Activar alertas de los movimientos con tarjetas, para llevar un mejor monitoreo de la actividad y detectar cualquier movimiento inusual.
6. Monitorear los estados de cuenta para identificar compras que no se hayan realizado, en caso de existir alguna, reportarla inmediatamente.
7. Destruir completamente las tarjetas de crédito o débito que ya hayan caducado.
8. Desactivar la opción Near Field Communication (NFC) de los dispositivos móviles mientras no se use, ya que esta tecnología permite conectar dispositivos para el intercambio de datos.
9. Utilizar las tarjetas virtuales que ofrecen los bancos para pagos online.
10. Cuando se reciba una tarjeta en el domicilio, es importante revisar que el sobre esté completamente cerrado y no presente indicios de haber sido abierto.
11. Contar con un porta-tarjetas antirrobo. Si se detecta algún tratamiento indebido de datos personales, puede reportarse ante el INAI.

Atentamente

Rubén Salazar Guerra y Sofía Solís Mora
Salazar & Solís Abogados, S.C.