

## **Asistencia jurídica de Allianz Partners recomienda prestar atención a los ‘carteristas digitales’**

**El uso de tarjetas bancarias como método de pago es uno de los más usados, en especial en vacaciones, debido a su seguridad y comodidad; sin embargo, su uso también entraña riesgos. Allianz Partners analiza los tipos de estafa online y ofrece distintos consejos para evitar posibles fraudes en tarjetas y cuentas bancarias**

Datos publicados por el Banco de España indican que durante el 2021 se realizaron 6.101 millones de operaciones de pago en terminales de punto de venta (TPVs), que frente a las 4.735 millones del 2020, representan un incremento de más del 128%. La seguridad y comodidad de este método de pago lo convierten en uno de los más usados. Sin embargo, también pueden sufrir ataques de ciberdelincuentes.

Según el equipo de Asistencia Jurídica de Allianz Partners, los nuevos métodos de estafa son cada vez más sofisticados y tienen el objetivo de obtener datos personales, cuyo uso indebido permite acceder, entre otras, a cuentas bancarias ajenas. Las técnicas de estafa más comunes son:

‘Phishing’: obtención de datos a través de correos electrónicos.

‘Vishing’: obtención de datos a través de llamadas.

‘Web spoofing’: obtención de datos a través de páginas web falsas.

‘Smishing’: obtención de datos a través de SMS.

‘Skimming’: obtención de datos copiándolos de la banda magnética de la tarjeta.

Paz Tejedor, responsable del departamento de Asistencia Jurídica de Allianz Partners, indica: "El mayor riesgo es el saldo en la cuenta corriente. Como primera medida de seguridad, conviene disponer de un saldo ajustado a nuestras necesidades y llevar el resto a otra cuenta no vinculada a la corriente".

Por otro lado, en caso de ser víctimas de una de estas técnicas, los expertos de la entidad recomiendan dar al banco la indicación de ‘no permitir descubiertos’, de modo que el importe defraudado se limite, como máximo, al disponible en cuenta, así como seguir los siguientes pasos:

**Bloquear la tarjeta bancaria:** Contactar con la entidad bancaria y comunicar los hechos, a fin de que

proceda al bloqueo de la tarjeta.

Denunciar los hechos: Este es un paso absolutamente imprescindible de cara a recuperar el dinero.

Reclamar la devolución: Se realiza ante la entidad bancaria, quien, no obstante, no tendrá obligación de proceder a la devolución del importe defraudado si considera que ha habido un incumplimiento o por negligencia de las obligaciones del titular.

En cuanto a la responsabilidad del usuario, el equipo de Asistencia Jurídica de la compañía aclara que está limitada. De manera que la entidad bancaria deberá devolver las cantidades que excedan dicho límite, sin embargo, agregan, que en este caso existen dos supuestos:

Que el titular nunca haya dejado de tener en su poder la tarjeta, por lo que el fraude se produce por duplicado o por sustracción de los datos de la misma.

Que se haya producido el robo o pérdida de la tarjeta con carácter previo al fraude. En este caso existe un límite de responsabilidad del usuario antes de la comunicación del robo o de la pérdida, cuantía que queda limitada a un máximo de 50 euros.

Paz Tejedor añade que "en términos generales comprar con el 'plástico' supone un alto grado de protección como forma de pago online; sin embargo, los nuevos 'carteristas' son más sofisticados y como usuarios debemos estar informados y atentos a nuestros datos y herramientas digitales".

**Datos de contacto:**

Beatriz Toribio  
+34 639 269 253

Nota de prensa publicada en: [Madrid, 10 de agosto 2022](#)

Categorías: [Nacional Finanzas E-Commerce Ciberseguridad](#)

---

**NotasdePrensa**

<https://www.notasdeprensa.es>