

Estafa viral: ¿se puede robar dinero con sólo acercarse a celulares y tarjetas contactless?

02/05/2025



Una broma que se volvió viral en redes sociales encendió la alarma entre miles de usuarios: un video muestra a una persona acercando un teléfono a bolsillos o mochilas y realizando supuestos cobros de dinero sin que las víctimas se dieran cuenta.

Según se ve en el video, la persona que acerca su celular a mochilas, tiene abierto en la pantalla un reproductor de sonido que simula el clásico efecto de cobro de un POS. Cada vez que se cruza con un transeúnte, acerca el celular a bolsillos, mochilas o carteras, activa el sonido y captura la reacción con una cámara oculta.

Algunas personas reaccionan con desconcierto. Otras no se dan

cuenta. En varias escenas, el autor del contenido simula huir tras el supuesto “cobro” invisible. La secuencia fue publicada en la cuenta de Instagram @ellocosebaszz y se viralizó en distintas plataformas.

El video disparó una pregunta concreta: **¿es posible robar dinero sin contacto físico a través de tarjetas o dispositivos con tecnología NFC?**

¿Se puede robar dinero con sólo acercarse a celulares y tarjetas contactless?

Gabriel Zurdo, especialista en ciberseguridad habló este jueves con **A24** sobre las estafas. Explicó que, para realizar un cobro, incluso uno sin contacto, se necesita contar con un **POS** (un cobro Point of Sale, se refiere a la transacción de pago realizada a través de un dispositivo electrónico en un punto de venta, generalmente usando tarjetas de crédito, débito o prepagas) **habilitado** que esté vinculado a una cuenta **destino de fondos**.

Es decir, cualquier intento de concretar una transacción debe pasar por un circuito formal y registrable. Lo que significa que sí, **el fraude es técnicamente es posible**.

Y marcó una diferencia técnica clave entre las **tarjetas físicas** y los dispositivos como **celulares** o **smartwatches**. En el caso de los celulares, el sistema requiere que el teléfono esté **desbloqueado** para que se pueda concretar un pago mediante **NFC**. Lo mismo sucede con los relojes inteligentes configurados con sistemas de pago como **Google Pay** o **Apple Pay**. Si el dispositivo está bloqueado, no se autoriza la operación.

«A ver, la tecnología NFC, que es Near Field Communication, Comunicación de Campo Cercano, es segura. Evolucionó», afirmó Zurdo.

Y aclaró: «Cuando vos usás el teléfono, el dispositivo tiene que estar desbloqueado. Y para la mayoría de las transacciones, hay un segundo factor de autenticación. La transacción te exige datos biométricos. Reconocimiento facial. O sea, cuando vos pagás con el celular, acercás el celular después de haberlo desbloqueado y te pide antes de hacer la transacción».

Sin embargo, sostuvo: «El año 2024 de fraude con tarjeta de crédito a nivel global fue de 35 mil millones de dólares y sigue creciendo. La proyección va al crecimiento. Las proporciones de por dónde se **ejecuta el fraude, en un 38% es por web**».

Mecanismos de seguridad implementados

Los pagos mediante dispositivos como celulares o smartwatches **requieren que el teléfono esté desbloqueado para que se pueda concretar la operación vía NFC**. Lo mismo aplica para relojes inteligentes configurados con sistemas de pago. Si el dispositivo está bloqueado, la operación no se autoriza.

Las tarjetas físicas no tienen este mecanismo de bloqueo por defecto, lo que podría permitirles transmitir información frente a un lector NFC.

Sin embargo, la comunicación entre la tarjeta y el lector se da mediante un protocolo cifrado. Este protocolo permite generar un código único para cada transacción (un identificador transaccional de un solo uso) que no puede repetirse ni reutilizarse para futuras operaciones. Además, ningún lector que no esté asociado a un adquirente autorizado puede canalizar una operación de forma válida.

Mastercard destaca que, durante el pago, la tarjeta no transmite información personal sensible como el nombre del

titular, el código de seguridad (CVV) o la dirección de facturación. También recordó que las tarjetas físicas tienen límites de monto para las operaciones sin PIN y, después de un número determinado de compras seguidas, el sistema bloquea los pagos contactless solicitando validación por código.

En cuanto a la responsabilidad ante un uso no autorizado, los usuarios cuentan con protección por responsabilidad cero, siempre que notifiquen al banco la pérdida o robo de la tarjeta.

Fuente: América 24