El robo invisible: cómo pueden vaciarte la billetera con solo acercarse a tu celular

23/02/2026

Los pagos sin contacto cambiaron para siempre la forma de pagar: basta apoyar el celular o la tarjeta y listo. Pero esa misma comodidad abrió una nueva puerta para el fraude digital. Una de las técnicas que más preocupa hoy a los especialistas es el llamado Relay Attack, un ataque que permite robar dinero sin tocar físicamente el teléfono de la víctima.

“El problema no está en el chip, sino en cómo usamos la tecnología”, advierte Facundo Balmaceda, especialista en ciberseguridad de SONDA Argentina, que sigue de cerca este tipo de amenazas.

En un contexto donde el efectivo pierde terreno frente a las billeteras virtuales y las tarjetas *contactless*, **la seguridad se volvió una carrera permanente** entre desarrolladores y ciberdelincuentes. Y el fraude por retransmisión NFC es uno de los desafíos más silenciosos.

A diferencia de los hackeos espectaculares que suelen verse en series o películas, este ataque no necesita romper sistemas complejos ni clonar tarjetas. Su fuerza está en **la cercanía y la velocidad.**

Los pagos sin contacto trajeron comodidad, pero también nuevas formas de fraude (Foto: Freepik)

“No estamos hablando de clonación, sino de un puente digital”, especifica Balmaceda. “Un atacante puede captar la señal NFC de tu tarjeta o tu celular cuando estás a apenas **cinco o diez centímetros**. Esa señal se envía por internet a otro dispositivo ubicado frente a un lector de pagos, incluso en otro país. Para el sistema, la tarjeta ‘está ahí’ y la operación se aprueba sin levantar sospechas”, explica el especialista de SONDA.

El eslabón más débil: el factor humano

Según el especialista, no se trata de una falla del hardware NFC, sino del **uso indebido de funciones legítimas que el propio usuario habilita sin notarlo**. Los atacantes no buscan vulnerabilidades masivas en los chips, sino permisos mal concedidos.

“El fraude se apoya en aplicaciones que parecen inofensivas”, señala Balmaceda. “Una linterna, una calculadora o una app cualquiera que pide acceso a NFC o a funciones de accesibilidad puede convertirse en la llave de entrada. **Cuando el usuario acepta sin leer, le entrega su billetera al delincuente**”.

Existen incluso herramientas creadas con fines académicos, como **NFCGate**, que hoy son aprovechadas por ciberdelincuentes. “No rompen nada: usan las APIs disponibles en Android y se apoyan en la distracción del usuario”, resume el experto de SONDA.

Caballos de Troya en el celular

El riesgo aumenta **fuera de las tiendas oficiales** de aplicaciones. Balmaceda cita estudios que muestran que muchas apps aparentemente simples piden decenas de permisos innecesarios.

“Es una táctica clásica. Se publica una app inofensiva y, tiempo después, se activa su comportamiento malicioso mediante una actualización”, explica. “Los lugares concurridos ayudan, pero **la puerta casi siempre se abrió antes, cuando el usuario instaló una app sin verificar su origen”.**

La ingeniería social, más que la tecnología, es el verdadero motor del fraude.

¿Quién responde cuando el robo ya ocurrió?

La responsabilidad es uno de los grandes puntos grises. En muchos casos, las entidades financieras sostienen que el usuario facilitó el ataque al instalar aplicaciones falsas. Para el especialista de SONDA, esa postura no alcanza.

“Si no hubo un consentimiento real, la operación es no autorizada”, afirma. “Trasladar **toda la culpa al usuario** frente a ataques tan sofisticados no parece sostenible, ni desde lo legal ni desde lo ético”.

Apagar el NFC, aclara, no es una solución de fondo. “Es una respuesta parcial y poco práctica”.

Señales de alerta: cuándo sospechar que el celular fue comprometido

No siempre hay una “alarma roja” que avise que algo anda mal. En ataques como el ***Relay NFC***, el teléfono puede no mostrar síntomas evidentes, porque el problema no está en el sistema operativo sino en una app maliciosa instalada previamente.

Aun así, Balmaceda detalla **comportamientos que deberían llamar la atención:**

- Consumo anormal de batería o de datos sin cambios en el uso habitual.
- Calentamiento del equipo incluso cuando no se lo está usando activamente.
- Permisos extraños en aplicaciones que no los necesitan, como acceso a NFC o funciones de accesibilidad.
- Mensajes o notificaciones inusuales vinculadas a pagos, “verificaciones” o supuestos problemas de seguridad.
- Movimientos financieros que el usuario no reconoce,

incluso por montos bajos o “de prueba”.

Android o iOS: ¿hay diferencias reales en el riesgo?

Existen diferencias entre plataformas, pero con matices. Para el especialista, el punto clave sigue siendo **el comportamiento del usuario**.

Android es un sistema más flexible y abierto, lo que también implica una mayor superficie de ataque. “**La mayoría de los casos documentados de relay NFC con malware se dieron en Android**, sobre todo por apps instaladas fuera de tiendas oficiales o con permisos excesivos”, explica Balmaceda. Bien configurado y actualizado, aclara, no es inseguro, pero sí requiere más atención.

En iOS, el ecosistema es más cerrado y los controles sobre NFC y permisos son más estrictos. Eso reduce considerablemente el riesgo de malware, aunque no lo elimina por completo. **“En iPhone, la principal amenaza sigue siendo la ingeniería social**: phishing, engaños y robo de credenciales”, señala.

En ambos casos, la conclusión es la misma: no es tanto la plataforma, sino cómo se usa.

El futuro: pagos más inteligentes

La clave, según Balmaceda, está en sistemas que analicen el contexto completo de la operación. “La autenticación contextual puede detectar incoherencias: un celular en una ubicación y el pago en otra, latencias extrañas o patrones atípicos. Y **la biometría debería ser obligatoria en cada transacción, sin excepciones**”.

El desafío, concluye el especialista de SONDA, no es tecnológico sino cultural. “El NFC y la inteligencia

artificial son herramientas poderosas, pero **siempre van a depender del factor humano.** Sin educación digital, no hay sistema que alcance”.

Fuente: TN