Qué es y cómo funciona el smishing, la nueva forma de estafa para acceder a tu celular

10/10/2025

No es noticia que los fraudes digitales evolucionan con la misma rapidez que las tecnologías que usamos a diario. Sin embargo, una de estas modalidades de estafa que más creció en los últimos meses, es el smishing, un tipo de ciberataque que utiliza mensajes de texto (SMS) como puerta de entrada para engañar a los usuarios y obtener acceso a sus datos personales, contraseñas e incluso a sus cuentas bancarias.

Este delito combina dos conceptos: **SMS** (mensajes de texto) y ***phishing***. De esa unión surge el término para nombrar a la estrategia que **aprovecha la confianza** que todavía genera esa tecnología en los usuarios para intentar vulnerar su seguridad.

Cómo funciona el *smishing*

El mecanismo es **simple pero efectivo.** Los delincuentes envían un **mensaje de texto** que aparenta ser de una entidad legítima, como un banco, una empresa de envíos, un organismo público o incluso un servicio de **streaming**, y que contiene un**enlace o un número de teléfono.** El objetivo es que la víctima, preocupada o interesada por el contenido del mensaje, haga click o responda.

Esta modalidad de fraude, que utiliza mensajes de texto para robar datos personales y financieros, no deja de crecer en Argentina.. (Foto: gentileza Kumparan)
Entre los mensajes más comunes aparecen:

- **Tu cuenta será suspendida, ingresá aquí para verificar tus datos.**
- Detectamos un inicio de sesión sospechoso, confirmá tu identidad.
- **Tenés un paquete pendiente de entrega, completa la siguiente información para retirarlo.**

Si el usuario cae en la trampa, es **redirigido a una página**

falsa diseñada para robar credenciales o, en el peor de los casos, **se descarga automáticamente un malware** en el teléfono que permite el acceso remoto al dispositivo.

Por qué es tan peligroso

A diferencia de otros intentos de estafa más fáciles de detectar, el *smishing* juega con dos factores: la **inmediatez** y la **confianza**. Los SMS suelen ser percibidos como más confiables que los correos electrónicos, y además aparecen directamente en la pantalla del celular, lo que genera una **sensación de urgencia.**

Los **ciberdelincuentes** saben que, ante la presión de perder acceso a una cuenta o no recibir un pedido, muchas personas actúan de **manera impulsiva y sin verificar la legitimidad** del mensaje.

De acuerdo con informes recientes de empresas de ciberseguridad, el *smishing* se convirtió en uno de los **métodos de fraude digital de mayor expansión a nivel mundial**. Millones de personas reciben estos mensajes a diario y, aunque muchos los eliminan de inmediato, un alto porcentaje interactúa con ellos.

En países como **Argentina**, donde el uso del celular es prácticamente universal, este tipo de ataques encuentra **terreno fértil.** A medida que aumenta la digitalización de trámites, compras y operaciones financieras, también crecen las **oportunidades** para que los estafadores exploten vulnerabilidades humanas y tecnológicas.

Cómo protegerse del *smishing*

Como en todos los casos de ciberseguridad, la **prevención** es la mejor herramienta. Algunas recomendaciones claves son:

- **No abrir enlaces sospechosos:** si llega un SMS con un link inesperado, lo mejor es no hacer click.
- **Verificar la fuente:** ante un mensaje que parece provenir de un banco, una tarjeta o una empresa, hay que comunicarse directamente con la entidad por los canales oficiales.
- **No compartir información sensible:** nunca hay que enviar **contraseñas**, números de tarjeta o códigos de verificación por SMS.
- **Activar sistemas de seguridad:** mantener el teléfono actualizado, utilizar autenticación en dos pasos y contar con un software de seguridad confiable.
- **Desconfiar de la urgencia:** si el mensaje presiona para actuar de inmediato, probablemente sea una estafa.

El *smishing* demuestra cómo la delincuencia digital se adapta constantemente a los hábitos de los usuarios. Hoy, el **celular** es mucho más que un medio de comunicación: es una **billetera**, una agenda, una oficina y hasta un canal de acceso a trámites oficiales. Esa concentración de datos sensibles convierte al dispositivo en el **blanco preferido de los estafadores.**

Cómo protegerse del *smishing*

Como en todos los casos de ciberseguridad, la **prevención** es la mejor herramienta. Algunas recomendaciones claves son:

- **No abrir enlaces sospechosos:** si llega un SMS con un link inesperado, lo mejor es no hacer click.
- **Verificar la fuente:** ante un mensaje que parece provenir de un banco, una tarjeta o una empresa, hay que comunicarse directamente con la entidad por los canales oficiales.
- **No compartir información sensible:** nunca hay que enviar **contraseñas**, números de tarjeta o códigos de

verificación por SMS.

- **Activar sistemas de seguridad:** mantener el teléfono actualizado, utilizar autenticación en dos pasos y contar con un software de seguridad confiable.
- **Desconfiar de la urgencia:** si el mensaje presiona para actuar de inmediato, probablemente sea una estafa.

El *smishing* demuestra cómo la delincuencia digital se adapta constantemente a los hábitos de los usuarios. Hoy, el **celular** es mucho más que un medio de comunicación: es una **billetera**, una agenda, una oficina y hasta un canal de acceso a trámites oficiales. Esa concentración de datos sensibles convierte al dispositivo en el **blanco preferido de los estafadores.**

Fuente: TN