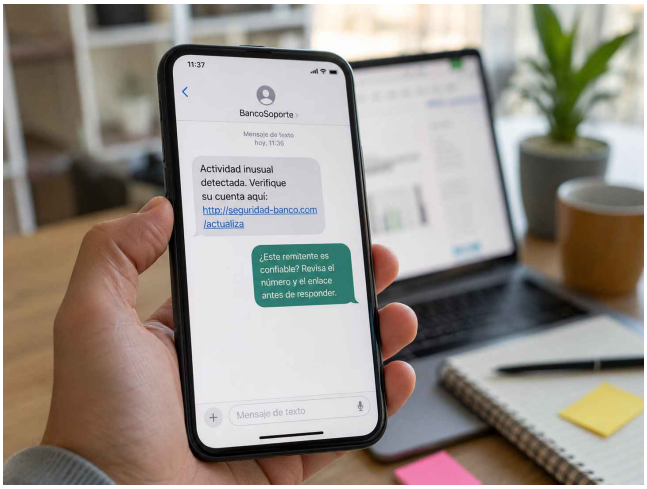
PANORAMA | Tecnología

El retraso del nuevo control de SMS mantiene la alerta frente a las estafas digitales

El bloqueo obligatorio de mensajes con alias no registrados se aplaza hasta el 15 de septiembre, por lo que habrá que mantener la prudencia ante posibles casos de smishing

Redacción/Priego Digital
Martes 2 de junio de 2026 - 10:52



La medida forma parte del plan para combatir las estafas de suplantación de identidad a través de mensajes fraudulentos. El Registro de Alias estará gestionado por la CNMC y afecta a los titulares de alias y a los proveedores de servicios de mensajería que envían mensajes identificados con esos nombres hacia números españoles.

El objetivo es reducir el smishing, una modalidad de fraude en la que los ciberdelincuentes envían mensajes simulando ser una entidad legítima, como un banco, una empresa de paquetería, una administración pública, una compañía telefónica o un comercio conocido. Normalmente, el mensaje incluye un enlace fraudulento o una petición urgente con la intención de robar datos personales, bancarios, contraseñas o códigos de verificación.

El retraso del bloqueo obligatorio implica que, durante el periodo de transición, conviene mantener la máxima precaución. Que un SMS muestre un nombre conocido como remitente no garantiza por sí solo que sea legítimo. Precisamente, los estafadores aprovechan esa apariencia de confianza para que la víctima actúe rápido, sin comprobar el origen real del mensaje.

La cuestión afecta también a pequeños negocios y entidades que utilizan SMS para confirmar citas, recordar reservas, avisar de pedidos, comunicar promociones, enviar códigos de acceso o mantener contacto con clientes. Clínicas, academias, gimnasios, talleres, asesorías, alojamientos, restaurantes, comercios online, asociaciones o entidades sociales deberían revisar con sus proveedores de mensajería si el alias comercial está correctamente registrado y si el servicio cumplirá con las nuevas exigencias a partir de septiembre.

Señales de alerta

Para el usuario, las señales de alerta siguen siendo claras: mensajes con enlaces acortados o extraños, faltas de ortografía, avisos de paquetes que no se esperan, supuestos pagos pendientes, amenazas de bloqueo de cuentas, promociones demasiado llamativas, peticiones de claves o solicitudes de códigos recibidos por SMS.

Ante la duda, la recomendación principal es no pulsar enlaces incluidos en mensajes sospechosos. Lo más seguro es entrar directamente en la web oficial escribiendo la dirección en el navegador, llamar al teléfono habitual de la entidad o consultar la aplicación oficial del banco, comercio o servicio correspondiente. INCIBE aconseja desconfiar de comunicaciones inesperadas, no responder a mensajes sospechosos y verificar siempre el remitente por canales oficiales.

También conviene recordar que ninguna entidad seria debería pedir por SMS contraseñas completas, claves bancarias, datos de tarjeta o códigos de verificación. Esos códigos son personales y no deben compartirse nunca, ni siquiera si el mensaje aparenta proceder del banco o de una empresa conocida.

Si se ha pulsado un enlace o se han facilitado datos, lo recomendable es actuar con rapidez: contactar con el banco, cambiar contraseñas, revisar movimientos, guardar capturas del mensaje y denunciar ante las Fuerzas y Cuerpos de Seguridad. En caso de duda, también puede recurrirse a la Línea de Ayuda en Ciberseguridad de INCIBE, el 017, disponible para ciudadanos y empresas.

La nueva regulación puede ayudar a cerrar una de las puertas más utilizadas por los delincuentes digitales, pero no sustituye a la prudencia individual. Hasta que el bloqueo obligatorio entre plenamente en vigor, el mejor filtro seguirá siendo el sentido común: desconfiar de la urgencia, verificar por canales oficiales y no entregar nunca datos personales o bancarios a partir de un SMS.