Gmail se despide del SMS: cuál es la nueva manera segura de autenticar las cuentas

25/02/2025

Google se moderniza y anunció que **cambiará el sistema de autenticación de Gmail** mediante SMS por otro basado **en un código QR** que se activará cuando el usuario pida ingresar a la cuenta. Esta modificación tiene como objetivo **frenar la amenaza que supone el abuso de los mensajes de texto y el hackeo de cuentas**.

Hasta el momento, **Gmail ofrece el envío de un SMS al celular del usuario como medida de autenticación** y se usa para confirmar que se trata de una persona legítima, enviando un código de inicio para poder validar la sesión.

Gmail. Foto: Unsplash.

Y aunque esto le añade una capa de seguridad al proceso de

verificación e inicio de sesión en la cuenta, el gigante de **la tecnología detectó que el abuso de este método puede facilitar los hackeos** debido a que es fácil acceder al número de teléfono de los usuarios e interceptar el código.

Por este motivo, según confirmó Forbes, **crearán un código QR con el objetivo de "reducir el impacto del abuso desenfrenado y global de los SMS".**

Gmail. Foto: Unsplash.

"En los próximos meses, vamos a repensar cómo verificamos los números de teléfono", indicó un portavoz de **Gmail** al medio citado anteriormente. "En concreto, en lugar de introducir el número y recibir un código de seis dígitos, **se mostrará un código QR que tendrás que escanear con la aplicación de la cámara de tu teléfono**", sentenció.

De esta forma**, se elimina la necesidad de recibir el código** y se reduce el riesgo de caer en una estafa de suplantación de identidad, mejor conocida como **phishing**.

Correo electrónico Gmail. Foto: Unsplash.

Qué es el phishing de cuentas de Gmail

El phishing es un tipo de fraude en línea en el que los delincuentes intentan obtener información confidencial, como contraseñas, números de tarjetas de crédito, datos bancarios, o cualquier otro dato personal, haciéndose pasar por una entidad confiable, como un banco, una tienda en línea o una red social.

El objetivo principal de esta práctica es **engañar a la víctima para que revele información sensible**, lo que puede ser utilizado para realizar fraudes financieros, robo de

identidad, o acceso no autorizado a cuentas.

Fuente: Canal 26