MásQueSeguridad

30 de marzo 2026

# LO MÁS RECIENTE

## >>> Alerta de "Quishing": El peligro oculto en los códigos QR físicos

Los ciberdelincuentes han perfeccionado una técnica híbrida llamada "Quishing" (Phishing con códigos QR). Están pegando calcomanías con QR maliciosos encima de los códigos legítimos en parquímetros, menús de restaurantes y paradas de autobús. Al escanearlos, la víctima es dirigida a pasarelas de pago falsas que clonan su tarjeta de crédito en tiempo real. Consejo: Si el código QR de un establecimiento público es una pegatina sobrepuesta, exige el menú físico o verifica la URL antes de ingresar cualquier dato.



## >>> Clonación de voz por IA: La nueva estafa de secuestro en WhatsApp

Con apenas 3 segundos de audio extraídos de un video de TikTok o Instagram, los atacantes ahora pueden clonar la voz de cualquier persona usando IA generativa. Están utilizando estas voces clonadas para enviar notas de voz desesperadas por WhatsApp a familiares, fingiendo un secuestro express o una emergencia médica y pidiendo transferencias inmediatas. Recomendación: Establece una "palabra de seguridad" secreta con tu círculo familiar íntimo para verificar la identidad en caso de emergencias monetarias.

## >>> Ransomware 2.0: Ahora los atacantes secuestran tus respaldos en la nube

Ya no basta con tener "copias de seguridad". Las nuevas variantes de Ransomware corporativo de 2026 están programadas para buscar y atacar directamente los repositorios en la nube (Google Drive, AWS, OneDrive) antes de encriptar la red principal de la empresa. Al borrar o secuestrar los respaldos primero, se aseguran de que las empresas no tengan más remedio que pagar el rescate.

@masqueseguridad | info@masqueseguridad.info | +58 424-2591446 | RIF.: J-0040984564-8