No abras esto en WhatsApp:

Las 5 ciberestafas que más víctimas han dejado en 2025

9 enero, 2026

Por Rubén García Deja un comentario

En 2025, **WhatsApp** ha vuelto a consolidarse como una de las autopistas preferidas para el fraude digital. No porque la app "sea insegura" por sí misma, sino porque su inmediatez, el tono cercano de los chats y la costumbre de responder rápido crean el escenario perfecto para la ingeniería social: confianza + prisa = menos verificación. Un repaso de Check Point identifica cinco patrones de estafa especialmente repetidos durante el año, con WhatsApp como canal principal o como "fase final" del engaño.

1) “Soy tu hijo/a”: urgencia emocional y transferencia rápida

El gancho suele ser simple: un número desconocido escribe afirmando ser un familiar (normalmente un hijo o hija) que ha cambiado de teléfono y necesita ayuda **ya**. La clave no es la historia, sino la presión: se empuja a actuar antes de comprobar. En cuanto la víctima entra en modo “rescate”, aparecen peticiones de dinero, bizums o transferencias con excusas creíbles (“me han bloqueado la cuenta”, “no puedo llamar”).

2) Ghost Pairing: secuestro “silencioso” de la cuenta

Aquí el objetivo es más ambicioso: tomar control de tu WhatsApp sin robar físicamente la SIM. Los atacantes intentan que la víctima facilite códigos o siga pasos que terminan vinculando la cuenta a un dispositivo controlado por el delincuente (aprovechando funciones legítimas como la vinculación de dispositivos). El usuario puede seguir usando su WhatsApp sin notar de inmediato que hay “un invitado” leyendo o enviando mensajes. Por eso este método es peligroso: permite suplantarte y, después, estafar a tus contactos desde una cuenta real y confiable.

3) Falsas notificaciones oficiales: multas, incidencias y “último aviso”

Otra táctica recurrente: mensajes que se presentan como comunicaciones de organismos públicos (por ejemplo, avisos de supuestas multas o trámites pendientes). El mensaje busca que pulses un enlace o que continúes la conversación por WhatsApp para “resolverlo” fuera de canales más controlados. El final suele ser el mismo: robo de datos, pagos indebidos o redirecciones a páginas falsas.

4) Suplantación de marcas conocidas: pedidos, cargos y cuentas bloqueadas

En esta variante, la máscara es una empresa popular (Amazon u otras plataformas de comercio y servicios digitales). El texto habla de un pedido retenido, un “cargo sospechoso” o una cuenta bloqueada y te guía a una web donde te piden credenciales o datos personales. A veces el daño va más allá del acceso a la tienda: el engaño se usa como trampolín para capturar información y, en algunos casos, para terminar comprometiendo la propia cuenta de WhatsApp o usarte como canal para seguir propagando el fraude.

5) La trampa “puente”: usar plataformas legítimas para terminar en WhatsApp

Las campañas más elaboradas empiezan en un entorno que inspira confianza (servicios o herramientas legítimas) y, cuando la víctima baja la guardia, el atacante cambia el terreno de juego y arrastra la conversación a WhatsApp. Check Point Research describe un ejemplo con invitaciones falsas que usaban Google Classroom como gancho inicial y, tras ese primer contacto, derivaban la interacción a WhatsApp, donde se remataba la estafa. El patrón es claro: sacar al usuario de un contexto con más señales y controles, y llevarlo a un chat rápido y personal.

Conclusiones y recomendaciones prácticas

La constante en estos cinco casos no es la tecnología, sino el comportamiento inducido: **urgencia**, **autoridad**, **familiaridad** y **cambio de canal**. Para reducir el riesgo:

- **Verificar por otra vía** (llamada normal, nota de voz, contacto alternativo) antes de pagar o compartir información.
- **Nunca compartir códigos de verificación** ni datos sensibles aunque el mensaje parezca venir de alguien "de confianza".
- Revisar **"Dispositivos vinculados"** y cerrar sesiones sospechosas; activar **verificación en dos pasos** en WhatsApp.
- Desconfiar de enlaces inesperados y evitar pulsarlos si no se puede confirmar su legitimidad.
- Mantener apps al día y usar opciones de seguridad adicionales disponibles en la plataforma.

Más información

- CyberSecurity News (28/12/2025): recopilación de las cinco ciberestafas más repetidas en WhatsApp durante 2025: https://cybersecuritynews.es/las-cinco-ciberestafas-de-whatsapp-que-mas-nos-han-timado-en-2025/