

Estas son las dos estafas por WhatsApp más peligrosas de 2025: te roban la cuenta y vacían tu homebanking

17/01/2025



WhatsApp es, sin dudas, una herramienta esencial para conectar a millones de personas en todo el mundo. Las personas la usan en el trabajo, para hablar con familiares e incluso para compartir contenido, como videos, stickers, fotos y más.

Sin embargo, su popularidad y gran adopción convirtieron a la plataforma en un blanco atractivo para los ciberdelincuentes, quienes constantemente desarrollan nuevas tácticas para engañar y estafar a usuarios desprevenidos.

A días de comenzado el 2025, **dos estafas ya son tendencia** en la plataforma por su peligrosidad y eficacia: el fraude de la oferta laboral y el engaño del falso [soporte técnico](#) de WhatsApp.



Estas son las dos estafas por Whatsapp más peligrosas de 2025: te roban la cuenta y vacían tus ahorros. (Foto: Adobe Stock)

El engaño del falso soporte técnico de WhatsApp

Este engaño es uno de los más **peligrosos y efectivos**. Se basa en la **manipulación psicológica y la ingeniería social**, donde los **delincuentes suplantan la identidad del equipo de soporte técnico de WhatsApp** para robar información de los usuarios, sus cuentas y acceder a sus [homebanking](#).

La estafa comienza con un **mensaje que parece legítimo, enviado desde un número desconocido** que a menudo tiene un prefijo internacional y una **foto de perfil igual al logo de WhatsApp**. Los estafadores se presentan como representantes del soporte técnico de WhatsApp, y le dicen a la eventual víctima que hay un problema con su perfil.

Un mensaje típico podría ser: **"Hola, hemos detectado que tu cuenta está siendo abierta en otro dispositivo. ¿Puedes confirmar que eres tú?"**. Otra versión es: **"Hola. Un cordial saludo desde soporte técnico de WhatsApp. Estimado usuario, le**

informamos que alguien recientemente se ha registrado en WhatsApp con su número”.

Este tipo de comunicación genera una sensación de urgencia y preocupación en las víctimas, quienes pueden sentirse obligadas a actuar rápidamente sin cuestionar la autenticidad del mensaje.

Cuando las víctimas responden al mensaje, suelen ser guiadas para confirmar su identidad con un simple “sí” o “no”, lo cual puede parecer inofensivo, pero es una trampa diseñada para obtener información valiosa: inmediatamente, **los delincuentes saben que el titular está del otro lado**.

En ese momento se pone en marcha la **segunda etapa, que puede darse de dos maneras diferentes:**

- **Mediante el envío de un link de descarga:** piden al usuario que instale una app y les pase el código de activación. Con ese número, los ciberdelincuentes pueden tomar control del celular de la víctima, capturar sus contraseñas y **acceder a su homebanking para vaciar sus cuentas** a través de transferencias.
- **A través del código de validación de WhatsApp:** los delincuentes intentan configurar el número de teléfono de la víctima desde sus dispositivos. La plataforma inicia el mecanismo de protección y le envía el titular un código numérico de seis cifras. Con diferentes excusas, los atacantes logran que el usuario les envíe ese número y así pueden **robar la cuenta de WhatsApp**.

A veces, **los estafadores realizan llamadas telefónicas en otra variante de esta estafa**. Así, le comunican a usuario que su WhatsApp fue abierto en otro dispositivo y le solicitan que le compartan un código de validación que les van a enviar al celular. Con la excusa de la urgencia, la víctima consulta las notificaciones en su smartphone, ve el número y se lo comparte

al delincuente. En ese momento, la comunicación se corta: su WhatsApp fue robado en ese instante.

El fraude de la oferta laboral

La otra técnica que es **tendencia en 2025**, tanto en WhatsApp como en Telegram, se basa en la **promesa de empleos atractivos** que, en realidad, son solo un señuelo para robar información personal o dinero a las víctimas.

Los estafadores envían **mensajes a través de WhatsApp que aparentan ser ofertas de trabajo legítimas**. Estos mensajes suelen incluir nombres de empresas reconocidas o agencias de empleo, creando una ilusión de credibilidad. Por ejemplo, pueden afirmar que están reclutando para compañías populares como Amazon, Mercado Libre, TikTok o YouTube, desde donde ofrecen **trabajos remotos con horarios flexibles y altos ingresos por tareas simples**, como ver videos, darle likes a publicaciones o escribir simples reseñas de comercios.

Una vez que la víctima muestra interés, los estafadores suelen solicitar información personal. En muchos casos, **se les pide realizar un pequeño pago “por gastos de gestión” o para recibir un “kit de inicio” para el trabajo**. Este es el punto crítico donde se consuma la estafa: tras enviar el dinero, los estafadores desaparecen y la víctima no solo pierde esa cantidad, sino que también puede ver comprometida su información personal.

Cómo detectar y evitar estas estafas

Para protegerse contra estas estafas, es **fundamental estar alerta y seguir algunas recomendaciones clave**:

- **Desconfiá de ofertas no solicitadas**: si recibís una

propuesta laboral inesperada por WhatsApp, es importante ser escéptico. Las empresas legítimas no suelen contactar a candidatos potenciales sin una solicitud previa.

- **Presta atención al lenguaje:** Muchas veces, los mensajes contienen errores gramaticales o un lenguaje poco profesional que delata su falta de autenticidad.
- Los mensajes del **soporte oficial de WhatsApp**, además de contar con el **tilde verde** de verificación, **no permiten responderle**, por lo que si está habilitada esa opción, se trata de una estafa.
- **No te dejes engañar por las fotos de perfil.** Cualquier persona puede usar la imagen que desee, incluso la de organismos oficiales y empresas reconocidas. **El avatar que use una cuenta de WhatsApp no es garantía de nada.**
- **Verificá el prefijo del número de teléfono desde donde te contactaron:** generalmente, si son de Nigeria (+234), Zimbabue (+263), Indonesia (+62), India (+91), o Marruecos (+212), desestímalos, ya que lo más probable es que sean llamadas spam o estafas.

Fuente: TN