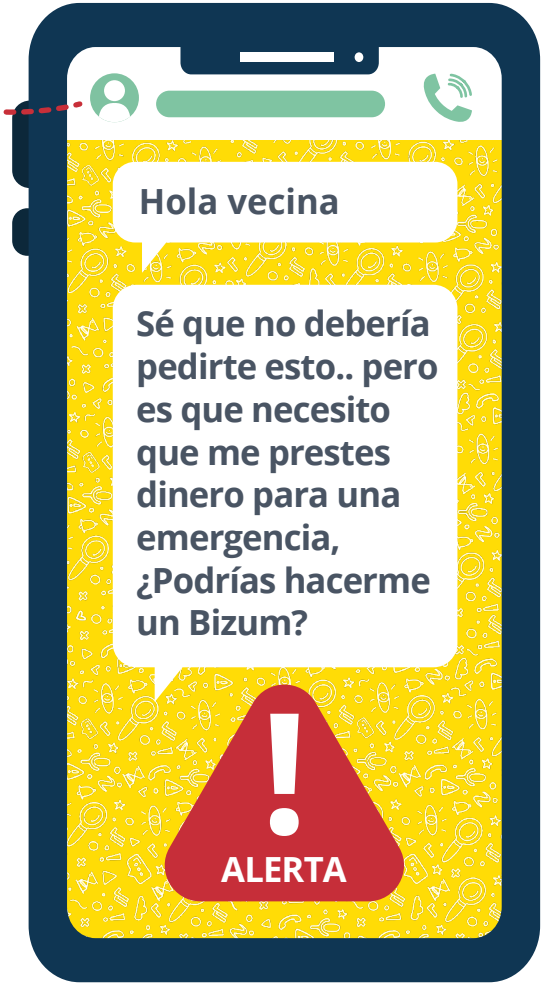
PRINCIPALES ESTAFAS POR WHATSAPP



WhatsApp es una de las aplicaciones que más utilizamos en nuestro día a día, por lo que debemos conocer **los riesgos a los que nos podemos enfrentar.** Los engaños más comunes se realizan mediante la suplantación de identidad **para solicitarte dinero,** aprovechándose de la confianza y la urgencia. Conociendo estos fraudes, podrás actuar con precaución y protegerte mejor frente a ellos.

¡Descubre cómo identificarlos y actuar frente a ellos!

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ESCENARIO 1

La estafa de la ‘maleta retenida’

¿En qué consiste y cuál es su objetivo?

Esta estafa es un engaño que aprovecha **las emociones y la confianza** de las personas para obtener dinero de forma fraudulenta. Los ciberdelincuentes **se hacen pasar por personas conocidas,** generalmente usando identidades falsas en este tipo de plataformas de mensajería instantánea, como WhatsApp. El objetivo es **pedir ayuda monetaria a la víctima, para poder recuperar una maleta** o propiedad que supuestamente ha sido retenida en un aeropuerto y que necesita con urgencia.

Paso a paso de la estafa

1. **Primer contacto:** los estafadores contactan con la víctima haciéndose pasar por alguien cercano. Para ello, suelen usar perfiles en redes sociales o información que hayan obtenido de alguna fuente pública o brecha de seguridad.
2. **Contexto emocional:** crean historias emotivas y urgentes para aumentar las posibilidades de engañar a la víctima.
3. **Supuesta retención de la maleta:** informan a la víctima de que la maleta está retenida por problemas de aduana o de transporte, y que para poder liberarla necesitan pagar unos impuestos o unas tasas, pero no pueden hacerlo porque guardaban el dinero o la tarjeta dentro de su maleta retenida.
4. **Solicitud de dinero:** solicitan un pago para que se realice lo más rápido posible, y con métodos que sean difíciles de rastrear como transferencias bancarias o servicios de envío de dinero. Además, prometen que devolverán ese préstamo rápidamente, tan pronto como puedan acceder a su maleta.
5. **Reiteración y presión:** en el caso de que la víctima responda de manera positiva, los estafadores pueden volver a pedir más dinero con otros pretextos u otros motivos distintos como pueden ser nuevas tasas o algún problema inesperado.
6. **Final:** una vez que han conseguido el dinero, los ciberdelincuentes desaparecen sin dejar rastro dejando a la víctima con una pérdida económica.

ESCENARIO 2

El fraude del hijo

¿En qué consiste y cuál es su objetivo?

Los ciberdelincuentes **se hacen pasar por un familiar** cercano, como un hijo/a, llamando desde un nuevo número de teléfono, alegando haber tenido problemas con el anterior, **para pedir dinero de forma urgente.** De esta forma, la persona que recibe este mensaje cree estar ayudando a un familiar en apuros, aunque en realidad estará realizando una transferencia o pago a un número de cuenta que proporciona el estafador.

Este fraude busca aprovecharse de la confianza generada al hacerse pasar por un familiar para engañar a la víctima. También hace uso de la necesidad de urgencia para que la víctima actúe sin poder pensar.

Paso a paso de la estafa

1. **Contactar con la víctima:** el ciberdelincuente contacta a través de WhatsApp desde un número desconocido, presentándose como un familiar (generalmente un hijo/a) y menciona que ahora tiene ese número debido a un problema con el anterior.
2. **Presentar una situación urgente:** una vez ha generado la confianza suficiente simulando ser un familiar cercano, el ciberdelincuente explica que se encuentra en una situación difícil y que le es imposible acceder a su dinero o contactos. Haciendo énfasis en que necesita ayuda de forma inmediata.
3. **Solicitar el dinero:** aprovechando la urgencia del momento, se pide enviar una suma de dinero para resolver el problema, proporcionando los datos bancarios o instrucciones de cómo realizarlo.
4. **Desaparecer o continuar la manipulación:** tras realizar la transferencia, en la mayoría de los casos, el estafador desaparece.
   Sin embargo, en algunos casos, puede seguir manipulando para solicitar más dinero o incluso información personal.

ESCENARIO 3

Falso soporte de WhatsApp

¿En qué consiste y cuál es su objetivo?

En este fraude, el atacante se hace pasar **por el soporte técnico de WhatsApp.** Los ciberdelincuentes contactan con la víctima informándole de que **su cuenta presenta un problema** o que está siendo utilizada de una forma indebida. Le solicitan al usuario que **comparta el código de verificación** que WhatsApp le envía por SMS al número asociado a su cuenta y lo justifican con pretextos, como puede ser **una verificación de seguridad** o algo necesario para comprobar la cuenta. También suelen alertar de que, **si no lo hacen, perderán su cuenta.**

Con este código pueden activar WhatsApp en otro dispositivo distinto. Si se le entrega al estafador, este puede obtener el control de la cuenta, mientras que el usuario legitimo se vería desplazado.

Paso a paso de la estafa

1. **Contacto con la víctima:** en este caso los ciberdelincuentes envían mensajes aparentando ser soporte técnico.
2. **Generar el código de verificación:** intentan registrar la cuenta de WhatsApp en otro dispositivo distinto, lo que genera un SMS con un código.
3. **Solicitar el código: l**e solicitan ese código a la víctima haciéndole creer que es necesario para solucionar un problema técnico o de seguridad.
4. **Toma de control:** una vez que estos reciben el código, acceden a la cuenta y la configuran en su dispositivo, incluso activando la verificación en dos pasos para bloquear cualquier intento de la víctima de recuperar la cuenta.
5. **Uso indebido:** a partir de ese momento los ciberdelincuentes pueden utilizar la cuenta para pedir dinero a otros contactos, extorsionar o realizar otro tipo de fraudes.

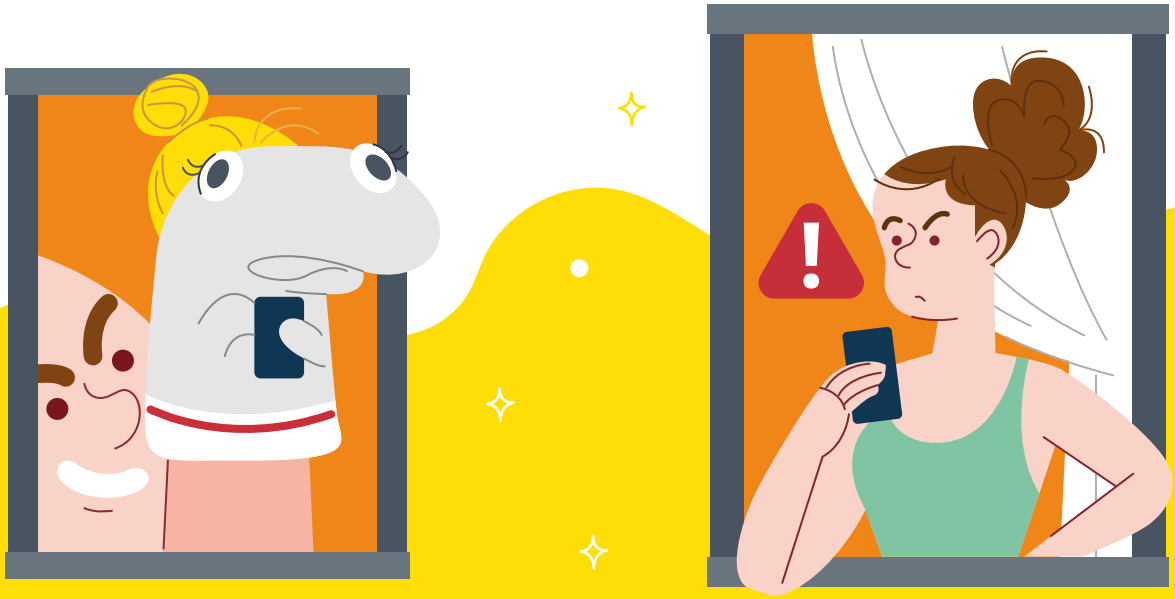
ESCENARIO 4

La estafa del falso vecino que se apoya en Bizum para engañarte

¿En qué consiste y cuál es su objetivo?

Consiste en l**a suplantación de un contacto conocido,** como un vecino a través de WhatsApp. Los ciberdelincuentes acceden a su cuenta tras un robo previo de su código de acceso y **envían mensajes a contactos pidiendo dinero con un pretexto urgente,** como problemas para realizar una transferencia mediante Bizum. Por lo que le ruega, incluyendo frases como "Sé que no debería pedirte esto..." para que realice el Bizum con la promesa de que el dinero será devuelto por la misma vía posteriormente.

El objetivo es obtener transferencias de dinero de forma inmediata, aprovechando la confianza entre vecinos, amigos o familiares, y continuar manipulando a la víctima para solicitar más dinero si el primer intento resulta exitoso.



Paso a paso de la estafa

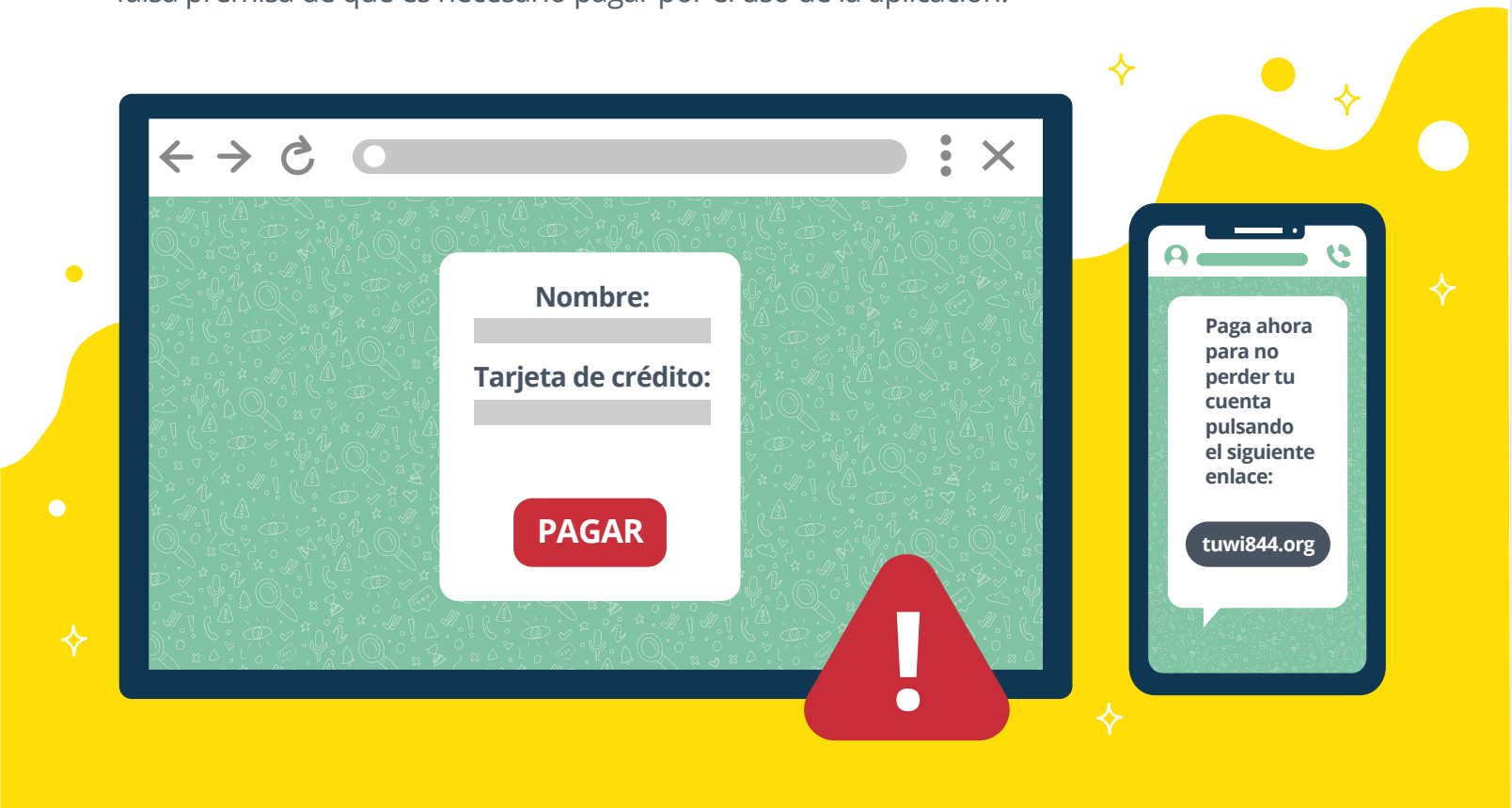
1. **Primer contacto:** tras acceder al WhatsApp mediante el robo del código de acceso, el ciberdelincuente escribe a diferentes contactos haciéndose pasar por el dueño de ese número, usando un tono cercano y preocupado por la situación para generar empatía.
2. **Solicitud de ayuda económica:** el estafador explica que necesita realizar un Bizum urgente, pero su aplicación o cuenta no está funcionando. Por lo que nos ruega que hagamos el pago y posteriormente cuando lo solucione lo devolverá.
3. **Proporcionar los datos de Bizum:** envía las instrucciones necesarias para realizar el pago, incluyendo un número de teléfono o una cuenta vinculada a Bizum. Puede incluir capturas de pantalla falsas o argumentos que refuercen la veracidad de la solicitud.
4. **Reclamar más dinero:** al realizar el primer Bizum, el estafador puede continuar solicitando una segunda transferencia con otra excusa o indicando que no es suficiente, dando la garantía de devolverlo todo junto.
5. **Desaparición del estafador:** una vez que el dueño original retoma el control de su cuenta, cualquier rastro del estafador se pierde, dejando a las víctimas sin posibilidad de rastrear o contactar a quien los engañó. Creando una situación confusa para ambas partes.

ESCENARIO 5

Pago falso para comprar la aplicación de WhatsApp

¿En qué consiste y cuál es su objetivo?

Busca engañar a los usuarios haciéndoles creer **que la aplicación es de pago** y que, en caso de no efectuarlo, **perderá acceso al servicio.** Para ello, el estafador proporciona un enlace a **una web falsa donde se solicita el pago** para supuestamente mantener activa la cuenta en esta plataforma.
De esta manera, los estafadores obtienen tanto las credenciales de pago como el dinero, sin que el usuario reciba nada a cambio. El principal objetivo es robar información financiera y cobrar bajo la falsa premisa de que es necesario pagar por el uso de la aplicación.



Paso a paso de la estafa

1. **Recepción del mensaje fraudulento:** se recibe un mensaje en dicha aplicación informando de que la aplicación ahora requiere un pago para seguir utilizándola. El mensaje a menudo menciona que el acceso al servicio se perderá si no se realiza el pago.

2. **Solicitud del pago:** el mensaje incluye un enlace que redirige a la víctima a una página fraudulenta que simula ser la página oficial o una tienda de aplicaciones. En esta página, se solicita realizar un pago para continuar usando la aplicación, pidiéndole que proporcione detalles de su tarjeta de crédito o que efectúe el pago mediante otros métodos en línea.

3. **Recolección de datos y desaparición del estafador:** tras realizar el pago, el estafador obtiene tanto el dinero como los datos bancarios de la víctima, pero no entrega el servicio prometido. Por último, el ciberdelincuente deja de contactar con la víctima, quien queda sin acceso al servicio y con el dinero perdido.

¿Cómo podemos evitar caer en estas estafas?

Desconfía de mensajes inesperados:

Si recibes un mensaje de alguien que no esperabas, verifica su identidad antes de continuar la conversación.

Analiza el lenguaje del mensaje

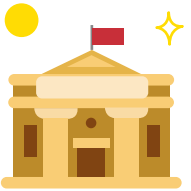
En este tipo de estafas se suele usar un español muy genérico, con errores ortográficos y expresiones que no usaría normalmente la persona a la que están suplantando.

Consulta directamente por otro medio a la persona en cuestión

Si dicen ser familiares o amigos, intenta contactar con ellos por otros medios.

Consulta a los organismos oficiales que se nombran

Si el problema es con aduanas o un aeropuerto, puedes verificar directamente este problema con el organismo correspondiente.



No compartas información personal ni bancaria

Evita dar detalles sobre tus cuentas bancarias o enviar dinero sin confirmar que el contacto es auténtico.

No compartas códigos de verificación

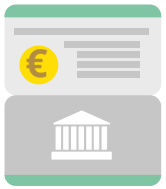
Ningún soporte técnico legítimo te pedirá que compartas tu código de verificación.

Medidas que puedes tomar si has sido víctima

Bloquea y reporta al estafador en WhatsApp: una vez identificado que el contacto es fraudulento, bloquea el número y repórtalo para evitar que pueda contactarte. De esta manera, investigarán el número y tomarán medidas, como eliminar la cuenta del estafador y prevenir que siga cometiendo fraudes en esa plataforma.

Denuncia el fraude: informa de lo sucedido a las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y reúne todas las evidencias disponibles, como conversaciones, mensajes, correos electrónicos, o números de contacto. Para obtener más detalles o asesoramiento, puedes comunicarte con la Línea de Ayuda en Ciberseguridad de INCIBE, marcando el 017. Este servicio es gratuito y confidencial, y también está disponible mediante chat en WhatsApp y Telegram.

Mantén un seguimiento en tus cuentas y contacta con tu banco: realiza periódicamente un seguimiento de tus cuentas bancarias afectadas para identificar cualquier movimiento sospechoso y contacta con tu entidad bancaria lo antes posible para bloquear dicha cuenta o tarjeta.



Practica el *egosurfing:* si has compartido información personal (como tu DNI, nombre completo, teléfono, etc.), realiza búsquedas periódicas en Internet para verificar si alguien está utilizando tus datos para suplantar tu identidad o llevar a cabo acciones indebidas. En caso de encontrar información no autorizada o incorrecta relacionada contigo, puedes ejercer tus derechos de acceso, rectificación, oposición y eliminación sobre el tratamiento de tus datos personales. La Agencia Española de Protección de Datos ofrece guías para ayudarte a realizar estos trámites.

Consejos y recomendaciones para evitar estos u otros fraudes similares.

- **Actualiza WhatsApp regularmente:** las actualizaciones suelen incluir mejoras de seguridad.

- **No pulses sobre enlaces sospechosos:** estos enlaces pueden contener código malicioso que infecte tu dispositivo o pueden abrir una página para descargar un archivo que contenga malware.

- **Activa la verificación en dos pasos:** añade un PIN adicional a tu cuenta desde la configuración de WhatsApp, este se solicitará siempre que se vaya a registrar esta cuenta en un nuevo dispositivo.

Para más información escanea el código:

O sigue este enlace:

https://www.incibe.es/ciudadania.