

TITULARES

Fraudes en los alquileres vacacionales

En verano se multiplica la demanda de alquiler de viviendas para vacaciones y, con el aumento de la demanda, también lo hacen los fraudes en los anuncios de alquileres vacacionales por Internet.

[Pág. 2](#)

Bizum inverso: una nueva estafa que puede costarte cara

Este tipo de estafa se basa en el engaño y la confusión como sus principales aliadas. En una operación normal de Bizum, una persona envía dinero a otra, pero en este fraude, el estafador envía una solicitud de dinero en lugar de un pago.

[Pág. 3](#)

Tu formación digital más fácil que nunca

Aprende Volando es un programa de formación diseñado para todas las personas, tengas la experiencia digital que tengas.

[Pág. 4](#)



Canal prioritario. Las redes sociales no son un juego

El [Canal Prioritario](#), de la Agencia Española de Protección de Datos, ofrece una vía rápida y gratuita para denunciar la publicación ilegítima en Internet de contenidos sensibles, sexuales o violentos, incluso sin ser la persona afectada.

Tú también **#PuedesPararlo**
con el **#CanalPrioritario**

Canal Prioritario

‘Las redes sociales no son un juego. Si compartes contenido sexual o violento perdemos todos’ es una iniciativa con la que la Agencia quiere poner el foco en la publicación en redes sociales de este tipo de contenidos y transmitir que todos podemos denunciar en el Canal prioritario su publicación.

EL POST-IT



LA PELÍCULA



CONTRAPORTADA

GLS no solicita confirmación de datos por correo para realizar una entrega



¿Has recibido un mensaje desde un número desconocido que dice ser tu hijo?



¿Puedes distinguir un audio real de uno hecho por IA?



¿Por qué es importante reiniciar el teléfono varios minutos al día para evitar ciberataques?



Comprueba si tu cuenta de correo está comprometida, <https://haveibeenpwned.com/>. Si es así, **cambia la contraseña.**

TITULARES

Fraudes en los alquileres vacacionales

Pistas para detectar [fraudes] en los alquileres vacacionales

En vacaciones, **mucho ojo con las ofertas y los alquileres vacacionales**. Los **ciberdelincuentes están al acecho** y debemos saber identificar los posibles fraudes.

¿Cómo podemos detectar estos fraudes?

Sigue estas pistas para destapar la trampa:

1

Fotos, fotos y más fotos:

Revisa atentamente las fotografías. Si hay pocas, son de mala calidad o son robadas de otro sitio... ¡que salten las alarmas! Estamos ante una posible estafa.

2

Ojo a la persona de contacto:

Si nos da poca información o pone pegajos para comunicarse en la plataforma y nos ofrece otras vías de comunicación o pago... No te la juegues.

4

Perfil investigador:

Saca la lupa e investiga. ¿Es la web segura? ¿Se repite el anuncio en más de una web de alquileres? ¿el dueño o arrendador es el original o cambia en otros anuncios?

5

Correos estafa:

¿Te llegan muchos correos de ofertas vacacionales sin haberte registrado en ninguna web? Revisalos con detenimiento y observa si utilizan un dominio gratuito. Puede tratarse de falsos anuncios.

¿Demasiado barato?:

¿Es demasiado bonito para ese precio? ¿Es el mayor chollo entre todos los que has visto? Desconfía. Los anuncios demasiado bonitos en zonas muy demandadas e imposibles de dejar escapar, suelen ser un fraude.

3

¡Sigue estas pistas y disfruta de unas vacaciones sin fraudes ni engaños!



Bizum inverso: esta nueva estafa puede costarte cara



La víctima, pensando que está aceptando un ingreso, en realidad está autorizando un envío de dinero al estafador, quien en su lugar ha enviado una solicitud de dinero. Al confirmar la operación sin revisar bien los detalles, termina perdiendo la cantidad especificada sin posibilidad de poder recuperarla fácilmente.

¿Cómo lo identifico y qué medidas puedo tomar?

❖ Señales de alarma:

- Si te contactan a través de una plataforma de compra/venta, es recomendable que **verifiques la información de esa persona en su perfil de usuario, además de su actividad y antigüedad en el sitio.**
- **La persona te insiste** en que aceptes un Bizum sin revisar los detalles, alegando **urgencia o alguna otra excusa para presionarte.**
- Vendes algo y el comprador acepta **pagar de inmediato**, sin hacer preguntas, intentar regatear ni mostrar interés en el estado del producto, incluso si el precio es elevado.
- **Mensajes extraños** o mal estructurados.
- Te contactan a través de **números desconocidos con ofertas demasiado buenas.**

❖ Medidas de prevención:

- **Revisa siempre antes de actuar** si se trata de aceptar un ingreso o si por el contrario es una solicitud de pago.
- Si alguien conocido te pide dinero por Bizum, **confirma su identidad a través de otro medio** como por ejemplo una llamada.
- Recuerda que **si eres el beneficiario de una transacción por Bizum no es necesario realizar ninguna acción**, el dinero llegará a tu cuenta sin ningún trámite por tu parte.
- **No compartas información personal o bancaria con desconocidos.**
- **Desconfía de ofertas demasiado buenas.**
- **Configura alertas en tu app bancaria** para recibir notificaciones sobre cualquier movimiento y activa la **autenticación de dos factores** si es posible.
- **No aceptes solicitudes de dinero de desconocidos.**

¿Qué hacer si has sido víctima?

En el caso de que hayas caído en esta estafa, debes actuar con rapidez para intentar minimizar el impacto y aumentar las posibilidades de recuperar el dinero que has enviado. Lo primero es entender que este fraude es muy común en plataformas de compraventa y que, como los pagos a través de *Bizum* no se pueden revertir, recuperar el dinero puede ser complicado. Sin embargo, a continuación, se presentan una serie de medidas que puedes tomar:

1. **Bloquea el número del estafador** para evitar que vuelva a contactarte.
2. **Reporta al ciberdelincuente en la plataforma de compraventa** para que puedan tomar medidas y evitar que siga estafando a más personas.
3. **Recopila todas las evidencias** posibles del fraude, como capturas de pantalla de los mensajes, detalles del pago y cualquier otra información relevante. Puedes hacer uso de '[Testigos online](#)' para certificarlas.
4. **Denuncia tu caso ante las [Fuerzas y Cuerpos de Seguridad del Estado](#)**, aportando todas las pruebas recopiladas.
5. **Contacta con la [entidad bancaria vinculada](#) a tu cuenta de Bizum y presenta la denuncia.** Ellos te indicarán los pasos a seguir y evaluarán si es posible tomar alguna medida para recuperar el dinero.
6. Si el banco no ofrece solución, **eleva la reclamación al Banco de España** para que evalúen el caso.

Si vendes productos en plataformas de compraventa o realizas pagos con Bizum, mantente alerta y aplica las medidas de seguridad recomendadas. En caso de haber sido víctima, actúa rápidamente siguiendo los pasos indicados para minimizar el daño y reportar el fraude.

La ciberseguridad es una responsabilidad compartida, y la información es nuestra mejor defensa.

Tu formación digital más fácil que nunca

Aprende Volando es un programa de formación diseñado para todas las personas, tengas la experiencia digital que tengas. Con cursos prácticos de 10 horas, vas a descubrir herramientas digitales que hacen tu día a día más fácil y te abren nuevas posibilidades, tanto en lo personal como en lo profesional.



Hemos preparado una selección de cursos sobre ciberseguridad, con distintos niveles y enfoques. Elige el que más te interese. **¡O hazlos todos!**

Uso seguro del correo electrónico

[Comienza ahora](#)

Contraseñas seguras: protege tus cuentas y dispositivos

[Comienza ahora](#)

Ciberseguridad esencial en el hogar

[Comienza ahora](#)

Protege tus redes WiFi

[Comienza ahora](#)

Protege a tus menores: control parental en el ordenador y en el móvil

[Comienza ahora](#)

El Programa de Formación “**Aprende Volando**” forma parte de la medida C19I1 “Competencias Digitales Transversales” en el marco del Plan de Recuperación, Transformación y Resiliencia y financiado por la Unión Europea-NextGenerationEU.

EL POST-IT

Fin del desempeño de las funciones

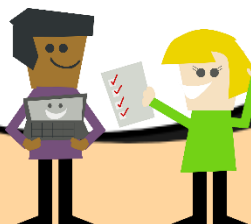
[Código de conducta](#) en el uso de las tecnologías de la información y la comunicación para profesionales públicos de la administración de la Junta de Andalucía.



Informa de las cuentas no personales que atendieras, en especial de correo electrónico y de redes sociales, y, en su caso, la contraseña cuando la hubieras creado tú o fueras su único depositario.

Relación de aplicaciones y sistemas que vinieras utilizando, en especial aquellas de otras Administraciones Públicas.

[Movilidad](#)



Cuando dejes de desempeñar las funciones que venías realizando o en caso de baja temporal que suponga una interrupción prolongada del desempeño de las mismas, para garantizar la continuidad del servicio, deberás comunicarlo a la persona responsable de tu unidad administrativa u órgano.

Relación de espacios de trabajo colaborativo en los que participas y los que administras.



Devolución de todos los dispositivos TIC que te hubieran sido asignados.



LA PELÍCULA



CONTAGIO

Los virus informáticos, al igual que los virus biológicos, tienen como objetivo contagiar cualquier sistema cercano, independientemente de su naturaleza.

Si el sistema no cuenta con defensas aceptables, el sistema 'cae' y en el peor de los casos 'muere'.



Antivirus



Bloqueo



Sospechas



Información

01. Antivirus

Dispón siempre de un programa antivirus y mantenlo actualizado.

02. Bloqueo

En el gestor de correo electrónico bloquea los archivos EXE, COM, PIF, SCR, VBS, SHS, CHM y BAT.

03. Sospechas

Sospecha de todos los archivos con más de una extensión, LOVE-LETTER-FOR-YOU.TXT.VBS

04. Información

Infórmate bien sobre las últimas amenazas de virus y ante cualquier duda, ponte en contacto con nosotros a través del correo electrónico o teléfono.

Correo: incidentes.soc@juntadeandalucia.es

Teléfono: 955 060 974

CONTRAPORTADA

GLS no solicita confirmación de datos por correo para poder realizar una entrega

Detectada campaña de correos electrónicos fraudulentos suplantando a la empresa de paquetería GLS. Se informa a la víctima que supuestamente tiene un paquete pendiente de entrega y para poder recibirlo debe acceder al enlace que se adjunta en dicho correo y confirmar los datos solicitados. Para más información, pulsa [aquí](#).



¿Has recibido un mensaje desde un número desconocido que dice ser tu hijo?

Detectada campaña de mensajes fraudulentos a través de SMS, en la que los ciberdelincuentes se hacen pasar por tu hijo o hija. Utilizan un número de teléfono desconocido y alegan que su móvil se ha roto, pidiendo que te comuniques con ellos a través de WhatsApp. El objetivo de esta estafa es engañar a la víctima para que realice un pago. Para más información, pulsa [aquí](#).



¿Puedes distinguir un audio real de uno hecho por IA?

Plataformas como Resemble Detect o AI Speech Classifier ya permiten comprobar si una voz ha sido clonada o si el audio ha sido creado con una aplicación concreta. Para más información, pulsa [aquí](#).



¿Por qué es importante reiniciar el teléfono varios minutos al día para evitar ciberataques?

Esta práctica cierra forzosamente cualquier aplicación y proceso que se esté ejecutando en segundo plano. Para más información, pulsa [aquí](#).

