CIBERCONSEJOS de Verano

CONSEJOS PARA EVITAR LOS FRAUDES DE VERANO

En verano se multiplica la demanda de arriendo de viviendas para vacaciones y, con el aumento de la demanda, También lo hacen los anuncios fraudulentos.Cada vez más personas deciden arrendar por Internet debido a sus numerosas ventajas: es más económico, rápido y tenemos a un solo clic muchísimas opciones. Lamentablemente las plataformas destinadas a este propósito, no están exentas de los intentos de fraudes por parte de los ciberdelincuentes.

¿Cómo funcionan estos fraudes?

Los estafadores se sirven de páginas web o aplicaciones especializadas en el arriendo de viviendas vacacionales, legales y fiables, para publicar ofertas de arriendo que resultan ser una trampa para los usuarios.

1. La trampa comienza con la creación de un anuncio falso, con fotografías robadas de otros anuncios y con una descripción y un precio muy atractivos. Este señuelo tiene como objetivo atraer el interés de las potenciales víctimas y al mismo tiempo generar confianza.

2. Otra opción muy utilizada por los ciberdelincuentes es la de enviar correos con enlaces de supuestas webs fiables, réplicas de otras plataformas más populares, pero que realmente son falsas. El objetivo es que acabemos compartiendo nuestros datos bancarios y demás datos de carácter sensible dentro de la web fraudulenta del ciberdelincuente.

Como usuarios, solemos dejarnos llevar por la sensación de estar frente a una gran oportunidad. Como consecuencia de esto hacemos un pago por adelantado para no dejar escapar la oportunidad. Sin saberlo, acabamos de ser estafados.

¿Qué podemos hacer para evitar este tipo de fraudes?

Desde CSIRT, hemos reunido algunos aspectos clave a tener en cuenta si queremos irnos de vacaciones tranquilos, sin caer en este tipo de fraudes.

1. Si encuentras anuncios muy atractivos y a un precio de escándalo, no te confíes. Muchos estafadores buscan atraer el interés de los usuarios por medio de fotos atrayentes, zonas muy demandadas o descripciones muy llamativas. Compara los precios del mercado con los de la oferta, y continúa con el resto de las recomendaciones.

2. Descripción con prisas. Si el anuncio publicado está mal redactado, tiene faltas ortográficas o se nota que ha sido escrito con prisas, es muy probable que nos encontremos ante una estafa. Es habitual que se utilicen traductores de texto automáticos que dejan los textos con errores o mal redactados. Lo mismo puede aplicarse a las comunicaciones con el arrendador.

3. Problemas y más problemas. Arrendar una vivienda en verano no debería ser una carrera de obstáculos. Es habitual que los anuncios fraudulentos solo muestren un correo electrónico y una vez recibidos los correos, los ciberdelincuentes contesten a los interesados desde otro email para dificultar su seguimiento. En ocasiones, también incluyen un teléfono de contacto, pero este siempre se encuentra apagado o no contestan.

4. Autenticidad del anunciante y del inmueble. Es muy importante comprobar la identidad del anunciante y de la titularidad y existencia del inmueble. Debemos ser conscientes de que la documentación puede falsificarse, incluso hay casos donde los estafadores utilizan las CI de otras personas que ya han estafado, apropiándose de su identidad. Pero también podemos emplear herramientas, como Google Street View para ver si nuestro departamento de ensueño existe, o comprobar desde Google imágenes, si las fotos del anuncio se han empleado en otras webs o plataformas diferentes.

5. Métodos de pago poco fiables. Es posible que el anunciante nos pida un adelanto para la reserva del alojamiento. Aunque no es una señal de alarma, debemos tener mucho cuidado con el método de pago que utilicemos. Si nos propone un método de pago alternativo a la plataforma, debemos desconfiar. Este tipo de webs disponen de plataformas de pago confiables con las que poder asegurar nuestras transacciones. Estos ciberdelincuentes recurren a métodos cada vez más sofisticados para conseguir su objetivo, es por ello que debes poner extrema atención a los detalles.

Por ello, siempre recomendamos seguir el sentido común para evitar este y otros tipos de fraudes. Si algo es gratis o demasiado atractivo desconfía y recuerda que en caso de dudas puedes ponerte en contacto con nosotros. www.csirt.gob.cl

Ministerio del Interior y Seguridad Pública
Gobierno de Chile
CSIRT
Equipo de Respuesta a Incidentes de Seguridad Informática
Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl

Síguenos en nuestras redes sociales
Infórmate sobre nuestras actividades y escríbenos directamente