Publicado en Madrid el 13/12/2022

# [Las tres estafas online más comunes en la Lotería de Navidad y cómo evitarlas](http://www.notasdeprensa.es)

## La Lotería de Navidad genera mucha ilusión y aporta felicidad a los afortunados que ganan alguno de sus premios. Sin embargo, también puede suponer una mala experiencia para quienes son víctimas de las estafas que los cibercriminales pertrechan aprovechando la fama de este juego. Los expertos de Kaspersky señalan las formas de estafa más comunes en torno a la Lotería de Navidad y comparten consejos para evitar caer en ellas

 Con la llegada de la Navidad, también vuelve a España una de sus principales costumbres: la Lotería de Navidad. No son pocas las personas que todos los años tienen como tradición comprar uno o varios décimos de lotería, habitualmente para compartir entre compañeros de trabajo, grupos de amigos o familiares. Los expertos de Kaspersky explican cuáles son las estafas más comunes que giran en torno a la Lotería de Navidad, y consejos para evitarlas. 1. Sitios fraudulentosLas estafas más comunes se dan en la compra de los décimos de Lotería a través de Internet. Muchas personas desean hacerse con un número concreto de la Lotería de Navidad y, al buscarlo online, pueden terminar en una web fraudulenta que les vende un billete que no existe o es falso. Para evitar ser víctimas de este engaño, los expertos de Kaspersky recomiendan: No caer en precios demasiado baratos o altos, ya que los cupones están regulados por el Estado y tienen un precio único de 20 euros, sin rebajas ni suplementos. Comprobar que el portal de venta al que se está accediendo es una web legítima. Para ello, hay que fijarse en la dirección web: los sitios fraudulentos no empiezan por https acompañado de un candado, que son los signos que aseguran que es una web autenticada y certificada. Guardar los mails de confirmación de compra. De esta manera, si se cae en la estafa, se podrán presentar los correos como prueba en caso de denuncia o incluso de juicio. Utilizar una solución de seguridad que impida que el dispositivo entre en estas webs. 2. PhishingEl phishing es una de las formas de fraude online más extendida. Se basa en el envío de mensajes a través de email o SMS, en el que se manda un enlace fraudulento para comprar alguna lotería o bien para directamente "cobrarla". El mensaje que se recibe captará la curiosidad de quien lo reciba, ya que, a menudo, aparece su nombre o dirección. Al pinchar en el link, se descarga un malware o virus que se introduce en el dispositivo de la víctima. De este modo, los expertos de Kaspersky recomiendan ignorar o eliminar el mensaje sin ni siquiera abrirlo, a ser posible. Otra forma de proteger los dispositivos de amenazas como el phishing, además de contar con una solución que brinde protección, es realizar el pago con seguridad. Se puede tramitar el pago a través de una tarjeta monedero en la que se introduce la cantidad de dinero necesaria para proteger el resto deahorros en caso de estafa. 3. Fraude en el cobro de premiosEn este tipo de estafas se utiliza la popularidad de premios como and #39;El Gordo and #39; para hacer creer a la víctima que es la empresa oficial de Loterías y Apuestas del Estado. En este caso, los estafadores envían un mensaje informando a la víctima de que ha ganado el premio y le ofrecen contactar con un agente. El supuesto agente solicita que rellene un formulario para verificar la identidad de la víctima a través de una copia del pasaporte o DNI. A continuación, normalmente a través de otro e-mail, se dan varias probabilidades para el cobro: transferencia bancaria, abrir una cuenta nueva en un banco desconocido o recoger el dinero personalmente en una localización lejana. El fraude ocurre cuando, antes de abonar el premio, se solicita un pago y, una vez hecho, los estafadores desaparecen. Los expertos de Kaspersky aconsejan tener muy en cuenta que estos mensajes casi siempre forman parte de un fraude por lo que, por lo general, lo mejor es ignorarlos o directamente denunciarlos. Para saber que estos mensajes son falsos, hay que poner especial atención al remitente: Las organizaciones oficiales no utilizan servicios de correo gratuitos como Hotmail o Gmail, si no que suelen tener un servidor propio. Si aún hay dudas de la veracidad del mensaje, se pueden utilizar los motores de búsqueda para verificar de dónde viene. Normalmente habrá otros usuarios que hayan caído en la trampa y hayan decidido compartir su testimonio en Internet. Lo más importante es recordar que si no se ha participado en ningún sorteo, es imposible que toque. Igualmente, soluciones de seguridad como Kaspersky Internet Security ofrecen la opción de activar el "Pago Seguro", herramienta que protege las operaciones financieras del usuario cuando visita la web de un banco, sistemas de pago y tiendas en línea. Funciona en cualquier página en la que se realicen pagos o se introduzcan los detalles de su tarjeta bancaria. "Los estafadores suelen aprovecharse de la expectación que generan determinados eventos, como el sorteo de la Lotería de Navidad, para estafar y robar dinero y credenciales a las víctimas que caen en sus trampas. El phishing, las webs fraudulentas y el engaño en los cobros de premios son las formas más habituales de engaño en torno a los juegos de azar. Por ello, es importante protegerse a través de soluciones de seguridad y de la propia cautela, siguiendo los consejos de los expertos", concluye Marc Rivero, Senior Security Researcher de Kaspersky.

**Datos de contacto:**

Mónica Iglesias

690196537

Nota de prensa publicada en: [https://www.notasdeprensa.es/las-tres-estafas-online-mas-comunes-en-la](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorias: Entretenimiento Ciberseguridad Premios



[**http://www.notasdeprensa.es**](http://www.notasdeprensa.es)