Publicado en Madrid el 29/10/2024

Kaspersky descubre ofertas fraudulentas del nuevo MacBook Pro con chip M4

Los expertos de Kaspersky han detectado una serie de estafas relacionadas con el lanzamiento de un nuevo modelo del MacBook Pro con chip M4, tras la publicación de una reseña de un influencer sobre este dispositivo aún no disponible. Aprovechando la expectación generada, los estafadores están ofreciendo preventas y programas falsos de prueba del portátil, con el objetivo de robar dinero y datos personales a los usuarios

Recientemente, un influencer ruso publicó una reseña en vídeo de un modelo no lanzado del MacBook Pro que incluye el nuevo chip M4, lo que generó rápidamente un gran revuelo en las comunidades de medios y tecnología, algo que los ciberdelincuentes aprovecharon para hacer el particular agosto. En este contexto, los expertos de Kaspersky han observado un aumento en las actividades fraudulentas, donde estafadores aprovechan la expectación ofreciendo preventas falsas y programas de prueba del portátil no lanzado, con el objetivo de robar dinero y datos personales de las víctimas.

Una de estas campañas de estafa se difunde a través de correos electrónicos, atrayendo a posibles víctimas con una oferta exclusiva para probar una nueva versión del MacBook, cuyo lanzamiento está previsto para noviembre. El correo contiene un enlace que, al acceder, redirige al usuario a una página web diseñada para imitar un mercado legítimo, prometiendo un portátil de prueba por tan solo 13 dólares, a cambio de proporcionar comentarios para mejorar el dispositivo. Para reclamar la oferta, los usuarios deben completar un formulario que solicita información sensible, incluyendo su nombre, dirección completa, número de teléfono y correo electrónico. Después de enviar los datos de contacto, se pide la información de la tarjeta de crédito para comprar el MacBook al precio exclusivo de prueba.

Como resultado, la víctima pierde dinero y, sin saberlo, envía detalles personales a los estafadores, con lo que se realizan retiradas no autorizadas de la cuenta. La información robada también puede venderse en foros de la Darknet, exponiendo a la víctima a robo de identidad y otros riesgos de privacidad.

Otra campaña de estafa implica una página web falsa de Apple. En primer lugar, piden a los usuarios que rellenen una breve encuesta, tras la que se informa que han ganado un nuevo MacBook gratis. A continuación, para reclamar el premio, les solicitan sus datos personales, como el número de cuenta, para cubrir los gastos de envío. Sin embargo, los usuarios nunca reciben el premio prometido y terminan perdiendo dinero.

"El vídeo publicado recientemente en el que aparece un portátil sin estrenar ha creado falsas expectativas, haciendo que la gente crea que, si un influencer ha conseguido obtener el dispositivo, también podría estar disponible para los usuarios. Los estafadores son rápidos en capitalizar las tendencias, sacando provecho de estos momentos para lanzar estafas aún más convincentes. Si algo parece demasiado bueno para ser verdad, probablemente lo sea. Siempre hay que verificar la información a través de las webs oficiales y evitar fuentes de terceros al realizar compras", comenta Dmitry Galov, jefe del Centro de Investigación en Rusia del Equipo de Investigación y Análisis Global

(GReAT) de Kaspersky.

Para evitar caer en estafas como estas, los expertos de Kaspersky recomiendan:

Limitarse a los canales oficiales. Solo comprar o reservar dispositivos Apple a través de las páginas web oficiales de los minoristas oficiales o partners de confianza. Evitar acceder a enlaces de webs desconocidas o correos promocionales, por muy atractiva que parezca la oferta.

Verificar las URL y direcciones de correo electrónico. Los estafadores a menudo crean páginas web falsas que son prácticamente idénticas a las legítimas. Siempre verificar que la URL comience con "https://" y coincida con el dominio oficial de Apple. Del mismo modo, tener cuidado con los correos electrónicos que provengan de direcciones sospechosas.

No compartir información personal. Desconfiar de cualquier web o correo electrónico que solicite información sensible, como los detalles de tarjeta de crédito, números de identificación personal o la contraseña de Apple ID. Apple nunca pedirá este tipo de información mediante correos electrónicos no solicitados o enlaces.

Utilizar una solución de seguridad fiable. Una solución de seguridad automatizada, como Kaspersky Premium, protegerá de todas las estafas, ya sean conocidas o no.

Datos de contacto:
Mónica
Kaspersky
690196537

Nota de prensa publicada en: Madrid

Categorías: Hardware Madrid Ciberseguridad Consumo Otros Servicios