LITORALPRESS

Fecha: 22-08-2024
Medio: Las Últimas Noticias
Supl. : Las Últimas Noticias
Tipo: Noticia general
Título: ¿Malvertising? Bancos alertan sobre anuncios falsos en sitios web

Pág. : 6
Cm2: 543,4
VPE: $ 2.988.403

Tiraje: 91.144
Lectoría: 224.906
Favorabilidad: No Definida

Descubra cómo los ciberdelincuentes utilizan este método para engañarlo

¿Malvertising? Bancos alertan sobre anuncios falsos en sitios web

IGNACIO MOLINA

¿Conoce qué es el malvertising? Es una forma nueva de ciberestafa donde los ciberdelincuentes introducen anuncios publicitarios fraudulentos en sitios legítimos de Internet.

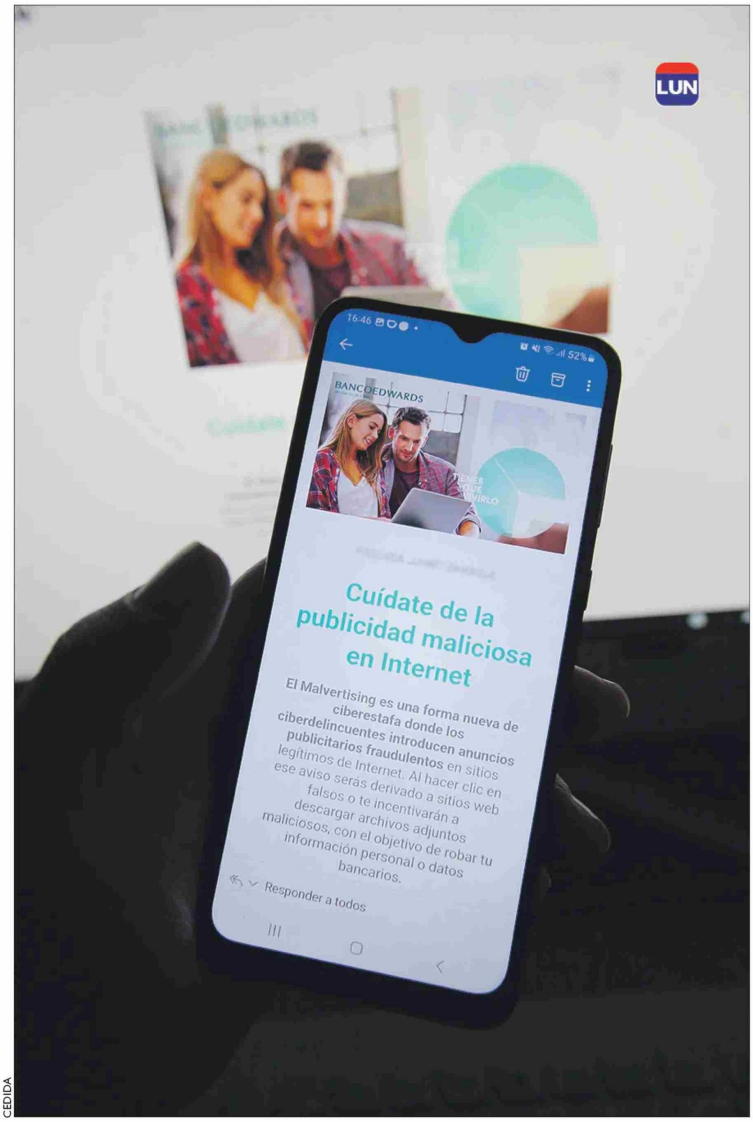
"Al hacer clic en ese aviso, serás derivado a sitios web falsos o te incentivarán a descargar archivos adjuntos maliciosos, con el objetivo de robar tu información personal o datos bancarios", advierte el Banco Edwards en un comunicado a sus clientes.

Sospeche si el aviso promete ofertas demasiado buenas para ser ciertas, como grandes descuentos, premios o regalos inverosímiles.

Gabriel Bergel, ingeniero en computación e informática, con magíster en ciberseguridad, detalla que el malvertising exactamente consisten en anuncios publicitarios falsos que tienen el único objetivo de invitar a un usuario a visitar un sitio web.

"Los hackers copian un sitio web completo (para hacerlo pasar, por ejemplo, por https://bancoedwards.cl), dice Bergel, presidente de la Fundación de Ciberseguridad 8.8. "Existen muchas plataformas gratis que no les permiten copiar un sitio completo y lo montan en una URL en otro país, en otro dominio, y simulan ser esa identidad para principalmente robar", añade.

Felipe Mancini, director ejecutivo de Asimov Consultores, empresa chilena que desarrolla apps móviles, software e inteligencia artificial, añade: "Estos anuncios parecen normales para el común de los usuarios, pero están diseñados para redirigir a los usuarios a sitios web falsos o para incitarlos a descargar archivos maliciosos. El objetivo de estos anuncios es engañar a los usuarios y robar su información personal, datos bancarios o infectar sus dispositivos con malwares".



CEDIDA

El objetivo del malvertising es robar su información personal o datos bancarios.

Cómo protegerse

¿Cuáles son las señales de alerta para identificar anuncios publicitarios fraudulentos en sitios web legítimos?

"Es fundamental estar atento a varias señales de alerta. Una de ellas es si el anuncio promete ofertas demasiado buenas para ser ciertas, como grandes descuentos, premios o regalos inverosímiles, o incluye testimonios de personas famosas que no parecen auténticos, lo cual puede ser un indicio de fraude", indica Mancini. "Otra señal es la redirección inesperada; si al hacer clic en un anuncio, eres llevado a un sitio web que no esperabas, esto podría ser un signo de que el anuncio es malicioso. Las URLs sospechosas, especialmente aquellas que no coinciden con la marca o el producto promocionado, son otra pista de que el anuncio podría ser fraudulento. Si, después de hacer clic en un anuncio, aparecen ventanas emergentes solicitando información personal o bancaria, es probable que se trate de un intento de malvertising", agrega.

Otro punto crucial, indica, es estar atento al comportamiento inusual del navegador, como la apertura automática de múltiples pestañas o ventanas (pop-ups o under ads). "Esto es un fuerte indicio de que estás interactuando con un anuncio malicioso", advierte.

Bergel, a su vez, afirma que los hackers, para atraer personas a esos sitios, pagan por poner los anuncios falsos en sitios web originales. "Generalmente, los sitios web no validan si el anuncio que están poniendo ahí es verdadero o no", dice.