



CIBERCONSEJOS DE SEGURIDAD para evitar los peligros del Malvertising

Cuando un anuncio es más que un anuncio

Como malvertising se conoce a un tipo de amenaza digital consistente en difundir programas maliciosos (malware) en avisos publicitarios falsos, pudiendo infectar a los usuarios incluso sin necesitar de que estos hagan clic en algún enlace.

QUÉ ES EL MALVERTISING



1. Cibercriminales esconden código malicioso en avisos de compañías de buena reputación, anuncios de falsos premios o formas fáciles de ganar dinero.
2. El objetivo es que los usuarios hagan clic en los anuncios, gatillando la descarga de programas maliciosos.
3. Para esto, los delincuentes inyectan avisos infectados en empresas de publicidad digital legítimas, o crean sus propias agencias falsas.
4. Peor aún, se venden kits para que los delincuentes puedan fácilmente implementar técnicas evasivas en sus avisos con códigos maliciosos.

MÉTODOS DE INFECCIÓN



1. Aparece un aviso, el usuario hace clic y su equipo es infectado con malware, el que puede robar datos personales, secuestrar sus sistemas (ransomware) o incluir el aparato en una botnet, entre otros.
2. A veces ni siquiera se necesita un clic: el malvertising puede estar incorporado en los scripts de la página y se ejecuta tan solo con visitarla.
3. También puede haber una infección con adware, programas que activan avisos indeseados en el equipo del usuario.
4. Muchas veces en lugar de anuncios, las imágenes son falsas advertencias de que el equipo tiene un virus u otro problema (scareware). La supuesta solución ofrecida por la advertencia suele ser un malware.

LOS RIESGOS DEL MALVERTISING



1. **Robar sus datos personales.** Los cibercriminales pueden utilizar malvertising para instalar spyware, que recopila sus datos personales y los envía al atacante.
2. **Extorsionar para pedirle dinero.** Si un anuncio infectado instala un ransomware en su equipo, es probable que se enfrente a un intento de extorsión. El ransomware bloquea sus archivos y exige el pago de un rescate para descifrarlos.

CÓMO DIFICULTAR SER VÍCTIMA



1. Conocer del malvertising y concientizar a otros sobre el problema.
2. Instalar programas antimalware y mantener actualizados sus sistemas.
3. Utilizar software que bloquean anuncios, conocidos como ad-blockers, que pueden impedir que avisos maliciosos descarguen malware al visitar una web infectada.
4. Utiliza un navegador seguro. Los navegadores seguros incluyen funciones especiales que te ayudan a mantenerte protegido frente a amenazas en línea como el malvertising.