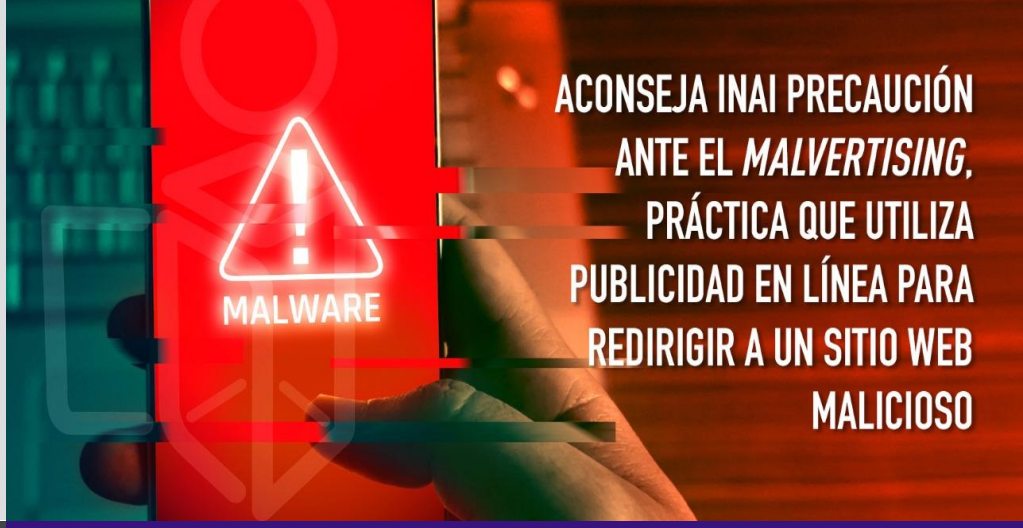
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

DIRECCIÓN GENERAL DE COMUNICACIÓN SOCIAL Y DIFUSIÓN

COMUNICADO • **INAI/231/22**



Ciudad de México.
30 de julio de 2022

www.inai.org.mx

- **Suelen ser anuncios que prometen grandes recompensas por completar un formulario o encuesta, dejar una reseña o realizar alguna otra tarea trivial para instalar malware en su dispositivo**

- **Otro tipo de ataques consiste en anuncios fraudulentos de soporte técnico, solicitando que llame a un número de teléfono, al hacerlo, se pondrá en contacto con un estafador**

ACONSEJA INAI PRECAUCIÓN ANTE EL *MALVERTISING,* PRÁCTICA QUE UTILIZA PUBLICIDAD EN LÍNEA PARA REDIRIGIR A UN SITIO WEB MALICIOSO

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) recomienda tener precaución ante la práctica de *Malvertising,* que consiste en el uso de publicidad en línea para difundir e instalar *malware* o redirigir a un sitio web malicioso, con el propósito de sustraer datos personales de las víctimas lo que podría resultar en usurpación de identidad, para pedir préstamos o cometer fraude.

El nombre *Malvertising* tiene origen en las palabras "*malicious advertising*" o publicidad maliciosa, término que describe la estrategia que siguen los atacantes, que utilizan sitios web confiables, ocultando el *malware* en ventanas emergentes, con el fin de infectar el dispositivo desde el que se está navegando.

Suelen ser anuncios que prometen grandes recompensas por completar un formulario o encuesta, dejar una reseña o realizar alguna otra tarea trivial. Al hacer *clic* puede remitirle a un sitio web malicioso o bien, descargar *malware* en su dispositivo.

Otro tipo de ataques hacen pensar al usuario que hay algo que funciona mal en su equipo con anuncios fraudulentos de soporte técnico que aparecen en el navegador mediante un código malicioso, solicitando que llame a un número de teléfono para obtener ayuda; al hacerlo, se pondrá en contacto con un estafador.

Existe otra estrategia que alerta, mediante ventanas emergentes, que el dispositivo ha sido infectado con un virus, y se le insistirá en descargar un *software* para resolver el problema, dicho archivo puede ser en realidad el *malware*.

Con el propósito de reducir la probabilidad de que las personas caigan en este tipo de engaños, el INAI emite las siguientes recomendaciones:

- Descargue siempre las actualizaciones de *software* desde el sitio web del fabricante.
- Instale un antivirus y verifique que siempre se encuentre activo y actualizado.
- Si algún anuncio le ofrece algo que parece demasiado bueno para ser verdad, no confíe.
- Previo a hacer alguna llamada a algún centro de atención, verifique que la empresa y el teléfono sean legítimos, y desconfíe si le solicitan datos personales, usuarios y contraseñas de cuentas, así como datos bancarios, más aún si son solicitados con sentido de urgencia.
- Utilice un bloqueador de anuncios, estas son herramientas diseñadas para ocultar o eliminar anuncios.
- Desactive los complementos de navegadores, como *plugins*. Puede ajustar la configuración de su navegador para limitar los complementos que se ejecutan de forma predeterminada.
- Mantenga actualizado su sistema operativo. Al utilizar la versión más reciente del sistema operativo, se reduce la exposición al *malvertising* dirigido contra vulnerabilidades antiguas y ya parcheadas.
- Utilice un navegador seguro y manténgalo actualizado. Los navegadores seguros y privados cuentan con una capa adicional de protección contra el *malvertising* y otras amenazas.

-o0o-

VER FOTOGRAFÍA