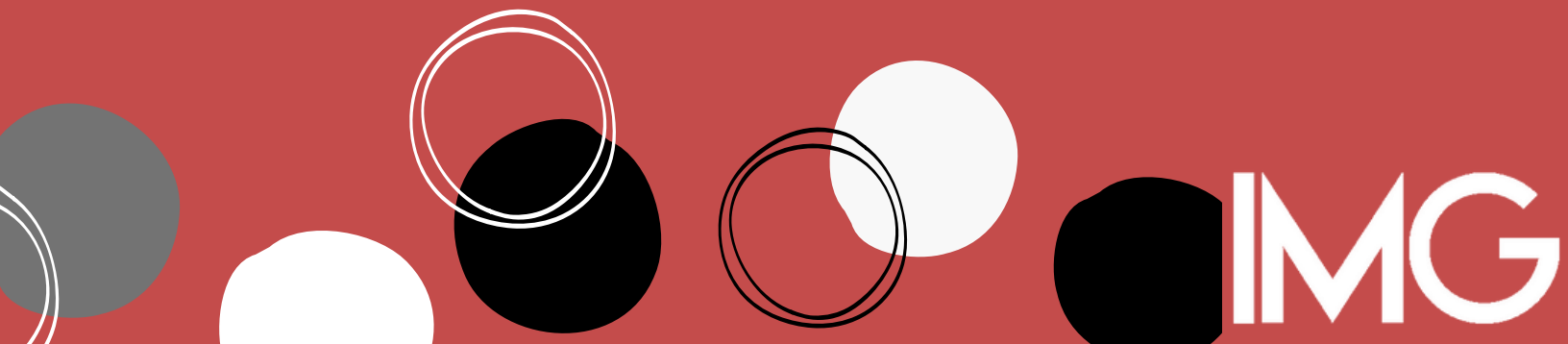




¿QUE ES EL SPYWARE?





¿QUÉ ES EL SPYWARE?

El spyware es un tipo de malware que roba datos de su dispositivo. Puede registrar lo que escribe, tomar capturas de pantalla e incluso usar la cámara de su dispositivo. Lea a continuación para obtener más información sobre qué es el spyware y cómo protegerse.

Algunos de los tipos más comunes

Información de tarjeta de crédito



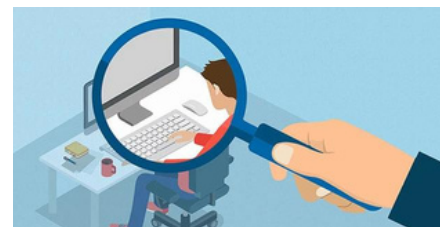
Credenciales bancarias



Contraseñas y nombres de usuario



Información sobre lo que haces en línea





¿CÓMO SE **INFECTA** TU DISPOSITIVO?

La forma más común de infectarse con malware es a través de archivos adjuntos y enlaces de correo electrónico. Muy a menudo, el software espía es un troyano y se instala en su dispositivo cuando instala otro programa. Debe tener especial cuidado con el software gratuito que se puede descargar en línea sin costo alguno. En realidad, estos programas aparentemente gratuitos pueden tener el precio de un software malicioso diseñado para monitorearlo y recopilar datos confidenciales sin su consentimiento.

Sin embargo, a diferencia de un virus o un gusano informático, los programas de software espía no intentan propagarse de un dispositivo a otro. Más bien, el spyware tiene como objetivo que el usuario lo instale sin que lo sepa.



¿SE PUEDEN INFECTAR LOS DISPOSITIVOS MÓVILES CON SPYWARE?

Aunque algunos podrían pensar que sus dispositivos móviles están a salvo de software malicioso, lamentablemente no es así. El spyware no es una excepción, ya que los dispositivos móviles también pueden infectarse con spyware.

Los mensajes de texto, por ejemplo, se pueden usar para infectar su teléfono inteligente con un programa espía malicioso. Una forma en que un programa de spyware puede llegar a su dispositivo es explotando la conexión Bluetooth del dispositivo.

Una buena manera de evitar el spyware móvil es **NO DESCARGAR SOFTWARE NI APLICACIONES DE TERCEROS**, ya que estos pueden incluir software malicioso no deseado. Utilice la tienda de aplicaciones oficial de su dispositivo, como Google Play y la tienda de aplicaciones de Apple, en su lugar. Asegúrese también de evitar archivos adjuntos de correo electrónico sospechosos, al igual que en su computadora.

EJEMPLO DE SOFTWARE ESPÍA:

PEGASUS (GRUPO NSO)



Es un conocido programa de software espía del Grupo NSO, una empresa de tecnología con sede en Israel.

Se dirige a dispositivos móviles que se ejecutan en los sistemas operativos iOS y Android.

Ha infectado dispositivos a nivel mundial desde su desarrollo en 2011.

El programa es capaz de eliminarse del dispositivo cuando se descubre.



5

CONSEJOS CONTRA EL SOFTWARE ESPIA

Como cualquier otro malware, no desea spyware en su dispositivo. A continuación, le presentamos 5 consejos de protección contra software espía que lo ayudarán a mantenerse seguro.

1 Utilice software antivirus

El antivirus bloquea el malware para que no infecte su dispositivo y lleva a cabo la eliminación automática de spyware.

2 Evita abrir enlaces y archivos adjuntos

Solo descargue y abra archivos y enlaces en los que confíe.

3 Evita abrir enlaces y archivos adjuntos

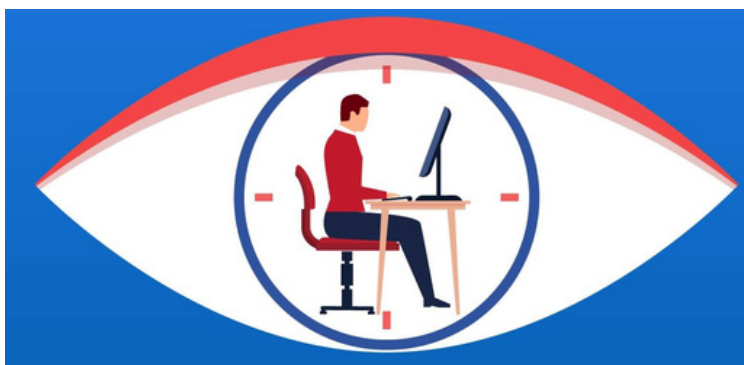
Solo descargue y abra archivos y aplicaciones en los que confíe. No descargue nada sin un antivirus activo. Esto se aplica tanto a dispositivos móviles como a computadoras de escritorio.

4 Mantén tu software y sistemas operativos actualizados

Habilite las actualizaciones automáticas en su computadora y teléfono para estar seguro.

5 No conceda a las aplicaciones permisos de dispositivo innecesarios

Puede editar los permisos ya otorgados desde la configuración de privacidad de su teléfono.



**PARA MÁS INFORMACIÓN
CONTÁCTANOS EN
NUESTRAS REDES SOCIALES**



IMAGENTI



TEL. 55127337

IMG