

TIPS LEGALES VENEZUELA

SEPTIEMBRE 2022



WhatsApp
Versie 2.12.13



Pishing en Whatsapp



¿Qué son los mensajes phishing?

El phishing es un ataque que intenta robar su dinero o su identidad, haciendo que divulgue información personal (como números de tarjeta de crédito, información bancaria o contraseñas) en aplicaciones o sitios web que fingen ser sitios legítimos

La forma en que los ciberdelincuentes utilizan WhatsApp para cometer algún tipo de fraude es muy variada y existen distintas modalidades. La mayoría de los engaños que circulan a través de la app o en su nombre utilizan la ingeniería social; es decir, el arte de manipular al usuario al hacerle creer algo que no es y convencerlo de que realice una acción que le interesa al delincuente.

Si bien muchas modalidades comparten características, repasamos algunas de las formas más comunes para cometer delitos como el robo de cuentas, suplantación de identidad o incluso distribuir malware:

- Engaño del falso aniversario de una marca
- Falsas ayudas económicas
- Engaños al azar para obtener datos personales
- Herramientas para espiar WhatsApp
- Secuestro de cuenta de WhatsApp
- Estafas de suplantación de identidad en WhatsApp
- Falsas actualizaciones con nuevas funcionalidades para WhatsApp
- Distribución de malware vía WhatsApp

Recomendaciones de Seguridad



Revisar las APKs de Whatsapp

La instalación no-autorizada de aplicaciones en el teléfono inteligente de los usuarios es uno de los procedimientos más repetidos en las estafas en Android.

Basta con que entremos en una página web con anuncios maliciosos para que, sin que seamos conscientes de ello, nuestro móvil descargue automáticamente un archivo APK que contiene una aplicación con dudosa finalidad. En muchos casos, los archivos APK que se descargan sin autorización del usuario corresponden a aplicaciones que tienen la capacidad de espiar el WhatsApp, y son una seria amenaza para la privacidad.

El procedimiento a seguir para detectar las amenazas más evidentes es el siguiente:

- Entrar en la aplicación de Ajustes de nuestro móvil.
- Después, entramos en el apartado de «Aplicaciones» (o «Administrador de aplicaciones»).
- Una vez dentro, después de habernos asegurado que tenemos seleccionada la pestaña de «Todas» (o «Todo»), desplazamos la pantalla hacia la parte en la que aparecen las aplicaciones que empiezan por la letra «W». Aquí, nos fijamos en que la única aplicación que aparezca sea la oficial de WhatsApp; si vemos cualquiera aplicación adicional ("WhatsApp Espía", "WhatsApp Spy" o "WhatsAppSPY", por mencionar los ejemplos más habituales), procedemos inmediatamente a su desinstalación.



Revisar las Conexiones que tenemos de Whatsapp Web

WhatsApp Web es una herramienta excelente para mantener conversaciones de WhatsApp desde el ordenador pero, al mismo tiempo, también resulta ser el punto más débil de la privacidad en WhatsApp.

Para evitar esta amenaza, lo único que debemos hacer es asegurarnos periódicamente de que no tenemos abierta ninguna sesión de WhatsApp Web en nuestra cuenta.



- Abrimos la aplicación de WhatsApp Web en nuestro móvil Android.
- Una vez dentro, pulsamos sobre el icono de los tres puntos que aparece en la parte superior derecha de la pantalla y, después, pulsamos sobre la opción de «WhatsApp Web».
- Ahora, después de la pantalla que indica el funcionamiento de esta opción, veremos un apartado con el nombre de «Ordenadores con sesiones abiertas». Si se nos aparece algún equipo, significa que alguien está accediendo a nuestras conversaciones desde otro dispositivo (a no ser que hayamos iniciado sesión recientemente desde el ordenador, en cuyo caso veremos los detalles de nuestro propio dispositivo); para poner fin a esa situación, pulsamos sobre la opción de «Cerrar sesión en todos los ordenadores». En el caso de que nuestro WhatsApp no pase de la pantalla que explica cómo funciona esta opción, significa que nadie está accediendo a nuestra cuenta mediante este método.

En WhatsApp Web para iPhone el procedimiento a seguir para detectar amenazas es similar:

- Entramos en la aplicación de WhatsApp de nuestro iPhone.
- Pulsamos sobre la pestaña de «Ajustes», ubicada en la parte inferior derecha de la aplicación.

Después, pulsamos sobre la opción de «WhatsApp Web». Si se nos muestra algún equipo activo, significa que alguien está teniendo acceso a nuestras conversaciones, de manera que pulsamos inmediatamente sobre la opción de «Salir de todos los equipos»; en caso contrario, estamos libres de espías (al menos desde este método).

3

Desconfía siempre de los mensajes sospechosos que contengan enlaces en WhatsApp,

incluso aunque sean nuestros contactos de confianza los que los envíen (pueden estar siendo víctimas de un secuestro de cuenta sin ser conscientes de ello).

4

Si recibes un mensaje SMS o un Whatsapp con el texto 'Saludos de WhatsApp' o 'Te envié un código de 6 dígitos por SMS por error. ¿Me lo puedes pasar?', bórralo inmediatamente

Si uno no se ha dado de alta recientemente de la aplicación, no ha solicitado código de verificación y recibe un mensaje con un código o enlace de verificación nunca comparta ese código con nadie ni haga click en ningún enlace, ya que de esta manera estará completando el proceso de alta del Hacker

Las víctimas reciben un mensaje de texto desde un número extranjero del cual se envía un Código 991-210 y un Link <https://v.whatsapp.com/991210?s=1>. Inmediatamente reciben un mensaje de un contacto de WhatsApp para que le reenvíe el código y después de unos segundos pierden el control de su WhatsApp a manos de quien envió el mensaje malicioso.

De ese modo se produce "un secuestro virtual", en que la persona que realiza el hackeo registra el número telefónico de la víctima en la aplicación de otro teléfono, accediendo a la sesión de WhatsApp pudiendo leer y enviar mensajes a su nombre, acceder a grupos, etc.

De igual forma si te **llaman** haciéndose pasar por trabajadores de las Compañías telefónicas o empleados de Whatsapp, solicitando datos a los usuarios o el código de 6 dígitos para actualizar la aplicación, es recomendable no facilitar ningún tipo de información personal o códigos por esta vía, porque siguen mismo procedimiento que en la estafa anterior.

Cómo recuperar una cuenta?...

Algunas de las víctimas pudieron recuperar su cuenta solicitando otro código de verificación y metiéndolo a toda prisa para recuperar el control de la cuenta. Si no funciona, lo más efectivo es ponerse en contacto directamente con WhatsApp para informar del robo.

Pishing en Whatsapp



El Servicio de Ayuda de Whatsapp, tiene los siguientes consejos de seguridad para proteger tu cuenta.

- Activa la verificación en dos pasos y proporciona una dirección de correo electrónico en caso de que olvides tu PIN.
- Nunca compartas tu código de registro ni el PIN de la verificación en dos pasos con otras personas.
- Establece un código para el dispositivo.
- Ten cuidado con quién tiene acceso físico al teléfono. Si alguien accede físicamente a tu teléfono, puede usar tu cuenta de WhatsApp sin tu permiso.

Te recomendamos que compartas estos consejos con tus familiares y amigos para ayudarlos a proteger sus cuentas de WhatsApp.

Nota: Si recibes un correo electrónico para restablecer el PIN de la verificación en dos pasos o el código de registro, pero no hiciste esta solicitud, no hagas clic en el enlace. Es posible que alguien esté intentando acceder a tu número de teléfono en WhatsApp.

¿Cómo usar la verificación en dos pasos para proteger tu cuenta?

La verificación en dos pasos es una función opcional que añade seguridad a tu cuenta de WhatsApp.

- Abre la pestaña de ajustes
- Selecciona la opción cuenta y allí la opción de verificación en dos pasos
- Toca activar
- Elige un PIN y escríbelo
- Confirma tu PIN
- Escribe tu dirección de correo electrónica y confírmala (agregar tu dirección de correo electrónico es opcional, sin embargo se recomienda hacerlo porque permite recuperar la cuenta más fácilmente)
- Nunca compartas tu PIN de verificación en dos pasos con nadie

¿Cómo podemos ayudarte?

Dejuris cuenta con experiencia y aliados expertos en asuntos penales, criminalísticos, tributarios, financieros, corporativos, laborales y civiles. Esto nos permite ofrecer una asistencia integral y de un gran valor agregado a su organización.



Douvelin J. Serra-González / Abogado LL.M

+ 58 412 3402150

+58 414 3594756

douvelin.serra@dejuris.net

[@dejuris_net](https://dejuris.net) [@serradouvelin](https://serradouvelin)