Fuente: OSI

Mensajería instantánea

El uso de programas y aplicaciones de mensajería instantánea es cada vez más usual en nuestro día a día. Al igual que otras herramientas basadas en Internet, debemos conocer qué riesgos podemos encontrar con este tipo de aplicaciones y qué soluciones adoptar para evitar problemas no deseados.

Protege tu identidad

Es habitual que las aplicaciones de mensajería instantánea en smartphones no pidan usuario y contraseña cada vez que las utilizamos. Esto significa que, en caso de pérdida o robo de un smartphone, la persona que se haga con el dispositivo puede enviar mensajes a todos los contactos de la víctima haciéndose pasar por ella.

Si detectas un comportamiento extraño de uno de tus contactos, te solicita información sensible, te pide un favor muy comprometedor, etc., **asegúrate de que esa persona es quien dice ser.**
Para evitar este problema debemos establecer una contraseña de bloqueo en el smartphone. Así impediremos que alguien que no conozca la contraseña pueda utilizar el dispositivo.

También debemos ser precavidos cuando hablemos con usuarios que no conocemos. La persona real con quien estamos intercambiando mensajes puede no corresponderse con la persona que aparece en la foto de perfil, ya que **cualquiera puede poner la foto de quien quiera**.

Cuando tengamos una conversación con un desconocido **no debemos facilitar información o imágenes personales**. Es la mejor forma de evitar que pueda ser utilizada de forma malintencionada.

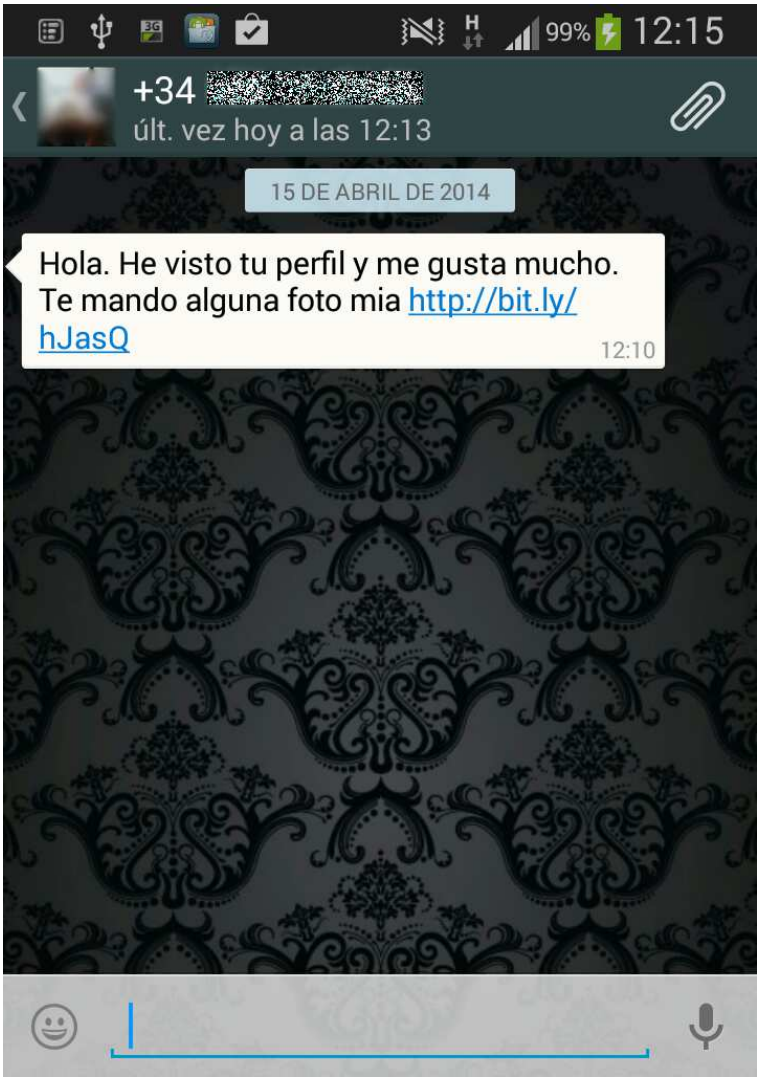
Existen virus en la mensajería instantánea

Los ficheros recibidos a través de aplicaciones de mensajería instantánea, sea cual sea el dispositivo, pueden contener virus. Éstos no solo afectan a los ordenadores, sino que también existen virus para tabletas, smartphones y todo tipo de equipos.

Normalmente los recibimos a través de ficheros adjuntos o aparecen en una conversación de chat a través de mensajes con un enlace que nos redirige una web maliciosa.

Debemos instalar un antivirus en todos los dispositivos que utilicemos, mantener el programa antivirus siempre actualizado y no aceptar archivos de contactos que no conozcamos.

Fuente: OSI



Protege a tus contactos

La práctica de crear grupos para el envío simultáneo de mensajes a varias personas puede resultar muy útil en aplicaciones como WhatsApp, Telegram o Line. Pero hemos de tener en cuenta que al crear un grupo, estamos difundiendo el número de teléfono de cada una de ellas al resto de miembros del grupo. Esto puede no ser conveniente en grupos de personas que no se conocen.

A día de hoy, las aplicaciones de mensajería instantánea no permiten la opción de ocultar los números de teléfono cuando creamos un grupo, como podemos hacer al enviar un email con copia oculta a muchas personas. Por ello, es conveniente asegurarse de que las personas que vamos a incluir en un grupo están de acuerdo y no se oponen a compartir su número de teléfono con el resto de miembros.

Fuente: OSI

Protege tus conversaciones

En general, las aplicaciones de mensajería instantánea almacenan el registro de las conversaciones en un fichero en el propio dispositivo, del que se hacen copias de seguridad. Esto incluye tanto el texto como los ficheros enviados y recibidos.

Cuidado con los archivos multimedia

Cuando recibimos un fichero multimedia a través de una aplicación de mensajería instantánea (fotos, vídeos, grabaciones de voz, etc.) no conocemos su contenido hasta que lo reproducimos.

Por tanto, existe la posibilidad de que, sin saberlo, reproduzcamos contenidos ilegales como fotos y videos de pornografía infantil, o que atenten contra la dignidad de una persona. Si los compartimos con otros usuarios, estamos **cometiendo un delito**.

Consejos finales

Si vamos a hacer uso de este tipo de aplicaciones, debemos aplicar una serie de recomendaciones:

- No difundas el número de teléfono móvil de otras personas sin su consentimiento.
- Instala un antivirus en el dispositivo (PC, tableta, smartphone) donde utilices la aplicación de mensajería instantánea.
- Asegúrate de que la persona con la que te comunicas es quien dice ser. No caigas en engaños.
- Establece una contraseña de bloqueo en tu dispositivo.
- Revisa siempre los ficheros que descargues. Ten cuidado de no difundir contenido ilegal.
- No facilites información privada. No sabes lo que tus contactos podrían hacer con esa información.
- Elimina el historial de las conversaciones con frecuencia. De esta forma evitarás que, si alguien accede al dispositivo de manera no autorizada, pueda leerlas y obtener información sobre ti que no deseas.
- Cuidado con las redes WiFi a las que te conectas para chatear. Si no están debidamente protegidas o son redes públicas, una persona malintencionada conectada a la misma red podría capturar tus conversaciones.
- Actualiza la aplicación siempre que aparezca una nueva versión por si ésta, además de incorporar alguna nueva funcionalidad, corrigiese algún fallo de seguridad.
- No te olvides de leer la política de privacidad y las condiciones del servicio antes de usarlo.
- Si la aplicación de mensajería instantánea que usas ofrece alguna opción de chat secreto, acostúmbrate a utilizarla.