MENSAJERÍAS INSTANTÁNEAS

SEGURIDAD Vs. USABILIDAD

**Si yo no soy Snowden ¿a mi qué me cuentas?**

Eso de que la seguridad en nuestras comunicaciones es importante lo hemos oído miles de veces pero no nos lo terminamos de creer. Confiamos en que nuestras comunicaciones diarias son tan poco interesantes que nadie se molestaría en interceptarlas, y entonces priorizamos la usabilidad sin mucha consciencia. Por supuesto que no tengo secretos tan relevantes como Edward Snowden y casi seguro que tú tampoco. Pero… haz memoria y repasa tus últimos mensajes, fotos, videos, contactos… ¿y si cayeran en manos de cualquier fisgónX? ¿O de algunX en concreto?. Las suplantaciones de identidad no son ciencia ficción, en serio: ocurren. (Recordemos que Zweerink ya inventó WhatsSpy Public). Eso de que la mensajería personal sea poco menos que magia para la mayoría… da miedito.

Quizá desde que el pasado año WhatsApp hiciera pública su decisión de compartir los datos con Facebook lXs usuariXs hemos empezado a pensar un poco. Ya todXs somos muy conscientes de que detrás de estas aplicaciones a las que estamos tan enganchadXs se encuentran multinacionales con intereses económicos y que nadie regala nada. Somos sus consumidorXs, no lo olvides. Hasta el momento hemos sido unXs valientes; hemos tragado con el texto plano, códigos cerrados, mensajes sin encriptar de extremo a extremo… Gracias a la aparición de nuevas aplicaciones como Telegram, Signal, Nepcom, Snaptchat, Line, Spotbros, WeChat, Wire, Viber, Google Allo, Hangouts… la seguridad en nuestras comunicaciones ha ido mejorando. Pero que no nos engañen: queda mucho por hacer.

Tenemos que ser más exigentes como usuariXs. Que les quede muy clarito a lXs programadorXs que necesitamos aplicaciones libres, justas y responsables. Como es lógico entre nuestra lista de contactos se hallan nuestras personas más queridas y no queremos que lo almacenen multinacionales, preferimos que lo hagan colectivos sin intereses pecuniarios. Que se enteren de que no nos gusta sufrir la presión por parte del servidor hegemónico de turno que nos obliga a utilizar su endemoniada aplicación porque es la que usa todo el mundo, que nos permitan de una vez comunicarnos entre usuariXs de distintas aplicaciones. Y que nos otorguen la libertad para modificar los códigos y protocolos. Deben garantizarnos de una vez por todas, la ansiada privacidad, que no se registre ni el contenido, ni los metadatos de nuestras conversaciones. Que a partir de ahora se obligue por ley a cada aplicación de mensajería instantánea un informe periódico de transparencia sobre qué tipo de información facilita a las autoridades o empresas. Amen.

**¿Nos conformamos con Signal de momento…?**

No es que lo diga yo, es que lo dice un ex agente de la CIA, que la App de mensajería instantánea más segura del mercado hasta el momento es Signal. Pero si yo estoy muy a gustico en WhatsApp que es dónde están todos mis amigos, ¿me quieres explicar por qué iba yo a descargarme otra aplicación que me pete el móvil?.

**Características de Signal que la hacen infranqueable:**

1. Encriptado de extremo a extremo. Así protege las conversaciones frente a terceros y frente al propio servicio.

2. No hay un servidor intermedio donde queden los mensajes. “Man in the middle”

3. Su encriptación cuenta con 256 bits. Dicen los entendidos que se necesitarían 1.000 años para entender su cifrado.

4. El código fuente no tiene puerta trasera. El cifrado de Signal es abierto. De tal manera que se puede comprobar su invulnerabilidad y los profesionales ajenos a la compañía pueden crear nuevas plataformas basadas en Signal

5. Permite establecer una contraseña para acceder al servicio como opción para obtener mayor seguridad

6. Los SMS de toda la vida se pueden enviar y recibir a través de Signal para mayor seguridad

7. Los mensajes pueden autodestruirse, a modo de Inspector Gadget. Entre 5 segundos y una semana.

8. Recortado de Mensaje. Esta opción eliminará automáticamente los mensajes más antiguos cuando la conversación exceda el límite de longitud especificado.

9. Sólo tienes que facilitar tu número de teléfono. No aportas mail ni tu nombre ni tu dirección física\*

**Pero alguna debilidad tendrá, ¿no?**

Pues sí. Como escribió Billy Wilder “Nadie es perfecto”. Una de sus citadas ventajas eso de que “sólo” facilitas tu número de teléfono no es más que una puerta abierta por donde pueden filtrarse más datos. Y es que para descargarte cualquier aplicación en tu móvil requieres tener instalado Google Play Services y para poder disfrutar de esa aplicación primero te has dado de alta en su base de datos. Así que sin quererlo ya estás fichada por Google. Además para que la mensajería de Signal funcione primero la aplicación manda un mensaje sin texto a través del Google Cloud Messaging (GCM) usando sus servidores. Así que a pesar de utilizar el encriptado de extremo a extremo ese primer mensaje vacío deja registro de los metadatos (quién habla con quién, desde dónde, cuánto tiempo). Y cómo os podéis imaginar muchas veces los metadatos son tan importantes como el propio contenido de la conversación.

Sin emparanoiarnos pero ya conocemos el historial de Google en colaboración con la NSA…

**Comparaciones odiosas y necesarias**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **WhatsApp** | **Telegram** | **Signal** | **Facebook Messenger** | **Nepcom** | **Skype** |
| **Usuarios** | Mil millones | 35 millones |  | 200 millones | Pocos. Tiene un año escaso! | 300 millones |
| **Países** | Sur de América, España, Italia, Alemania, Polonia, | Irán y Uzbequistán. Su uso crece en Brasil y España |  | Norte de América, Australia, Francia, Portugal, GB y Suecia | España | Antigua URSS |
| **Encriptado de extremo a extremo** | Sí | Sólo en chat secreto | Si | No | Sí | No |
| **Archivos** | Sí | Sí. Hasta 1,5gb | No | Sí | Sí |  |
| **Se puede verificar la identidad del contacto?** | Si |  | Sí |  |  | No |
| **El código es abierto?** | No | Sí | SI | No |  | No |
| **¿Si te quitan las claves están a salvo tus mensajes?** | Sí |  | Sí |  |  |  |
| **Stickers** |  |  |  |  |  |  |
| **GIF animados** |  |  |  |  |  |  |
| **Dispositivos** |  |  |  |  |  |  |
| **Notas** |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**SIGNAL PIRVATE MESSENGER**

Esta App de mensajería instantánea nace en 2014 de la mano de OpenWhisperSystems y su fundador Moxie Marlinspike, que fusiona en Signal sus dos aplicaciones anteriores Redphone y Textsecure. Su pasado anarquista no le ha impedido aceptar cargos como jefe de tecnología de Twitter, desarrollar la encriptación punto a punto de Whatsapp, o trabajar para Apple. Lo que hace especial a esta aplicación es que OpenWhisperSystems no basa su negocio en la publicidad y no vende sus datos a terceros (o eso dice). Permite mensajería, llamadas, sms y mms. Disponible para Android o iOS y se espera una versión para tabletas. Si queremos usarla desde el ordenador, existe una extensión para Chrome que permite enlazarla mediante código QR.

Fuentes:

<https://www.efe.com/efe/espana/portada/el-centro-criptologico-del-cni-alerta-sobre-los-riesgos-uso-whatsapp/10010-3060896>

<http://internacional.elpais.com/internacional/2013/08/23/actualidad/1377272049_738995.html>

<http://www.androidpit.es/aplicaciones-alternativas-whatsapp>

<https://www.tutecnomundo.com/las-aplicaciones-mensajeria-mas-seguras-android/>

<https://blog.kaspersky.com.mx/mensajeria-segura-en-internet-es-una-ficcion/2858/>

<http://www.elmundo.es/tecnologia/2017/01/13/5878fcaf468aeb38628b463c.html>

<https://www.osi.es/actualidad/blog/2014/05/09/whatsapp-telegram-y-line-cual-es-mas-segura-para-chatear>

<https://www.xataka.com/seguridad/como-funciona-el-cifrado-extremo-a-extremo-de-whatsapp-y-que-implicaciones-tiene-para-la-privacidad>

<http://geek.com.mx/2016/05/whatsapp-vs-telegram-vs-signal-que-es-mas-seguro/>

<https://es.wikipedia.org/wiki/Signal_(software)>

<http://computerhoy.com/paso-a-paso/apps/como-funciona-signal-alternativa-whatsapp-mas-segura-52034>

<https://cincodias.elpais.com/cincodias/2016/05/10/lifestyle/1462894604_072508.html>

<http://www.cromo.com.uy/ojo-los-chats-la-debil-seguridad-la-mensajeria-n670776>

<https://www.jabberes.org/>

<https://www.efe.com/efe/espana/portada/el-centro-criptologico-del-cni-alerta-sobre-los-riesgos-uso-whatsapp/10010-3060896>

<http://www.eldiario.es/cultura/privacidad/Messenger-Danger_0_603340331.html>

<http://www.panamaon.com/noticias/tecnologia/15465-nepcom-la-app-de-mensajeria-instantanea-corporativa-que-autodestruye-datos-confidenciales.html>

<http://www.tendenciasguate.com/2015/01/los-4-sitios-porno-mas-populares-entre.html>