Privacidad en Internet y condiciones de uso en Google, Facebook y whatsapp

Privacy in Internet and terms of service in Google, Facebook and Whatsapp

Salvador Barrera Rodríguez
Universidad de Guadalajara
sadvalor@tutanota.com

Resumen:

Ante el auge de las redes sociales, la mensajería instantánea, servicios de computo en la nube y la revelación de información privada, este articulo pretende formar conciencia "del comportamiento público en Internet", qué medidas se pueden tomar para proteger la privacidad, la seguridad de la contraseñas, para depender menos de soluciones gratuitas donde los usuarios son el producto y son rastreados por publicistas, terceras partes y gobiernos. Analizando las políticas de sitios populares como Google, Facebook y Whatsapp, reconociendo sus puntos débiles, recomendado medidas para fortalecer la privacidad y realizar algunas recomendaciones prácticas para fortalecer la privacidad.

Palabras Clave: Privacidad, Redes sociales, Computo en la nube, Mensajería Instantánea.

Abstract

With the growth of social networking, instant messaging, cloud computing and disclosing private information, this article aims to develop awareness "of public behavior on the Internet", what steps can be taken to protect privacy, security the passwords, to reduce dependence on free solutions where users are the product and are tracked by advertisers, third parties and governments. Analyzing policies popular sites like Google, Facebook and Whatsapp,

recognizing its weaks points, recommended measures to strengthen privacy and make some practical recommendations to strengthen privacy.

Key words: Privacy, Social Networks, Cloud computing, Instant Messaging

Introducción

¿Por qué la privacidad importa?, ¿si no se tiene nada que esconder?. (Greenward, 2014) Tiene una conferencia donde explica, que si no importará la privacidad, no habría necesidad de contraseñas, llaves y candados. Además puede que en este momento no quiera ser activista por una causa, pero eso no debe limitarnos de poderlo hacer en el futuro. Y sobre la pregunta del inicio del párrafo el autor opina:

> *"una pregunta que ha surgido en el contexto de un debate global activado por las revelaciones de Edward Snowden de que EE. UU. y sus socios, sin el conocimiento del resto del mundo, ha convertido internet, aun siendo reconocida como herramienta de liberación y democratización sin precedentes, en una zona sin precedentes de vigilancia masiva e indiscriminada."*

El autor es un periodista que ha trabajado con Edward Snowden y también comenta:

> *"Lo que realmente dicen es: "Estoy a favor de hacerme una persona tan inofensiva, tan poco intimidante y tan poco interesante que realmente no puedo temer que el gobierno sepa lo que estoy haciendo". Esta mentalidad ha encontrado lo que creo que es su expresión más pura en una entrevista del 2009 con el director de Google, Erich Schmidt, quien, cuando le preguntaron sobre las varias formas en que su compañía incurría en invasiones de privacidad de cientos de millones de personas en todo el mundo, dijo esto: "Si estás haciendo algo que no quieres que los demás sepan, tal vez, en primer lugar, no deberías hacerlo"."*

Los ámbitos donde más debemos cuidar la privacidad, es en el uso de las redes sociales, la mensajería instantánea, el almacenamiento en la nube y el uso de los teléfonos celulares como lo

proponen (Amaro, 2013), (Bernhard Debatin, 2009), (Iulia Ion, 2011), (Martijn, 2013), (Na Wang, 2011), (Tello-Díaz, 2013), (Thomas, 2010).

Sobre la idea de que el uso del teléfono celular crear un espacio virtual que permita hablar temas privados, aunque se encuentre en espacios públicos menciona: La Rosa, A. (2011) citada por (Amaro, 2013) describe:

> *"Las personas hablan sin ningún inconveniente sobre su vida privada y sus intimidades a través del teléfono móvil, al lado de desconocidos, como si estos no existieran ni escucharan. Paradójicamente su móvil les otorga la sensación de privacidad, la cual no existe pues la única vinculación existente está dada por el espacio que comparten momentáneamente. En este "compañerismo temporal" la distancia social tal vez íntima, no expresa lazo afectivo alguno entre los participantes"*

De ahí pasando a la mensajería instantánea a través de la aplicación Whatsapp (Martijn, 2013) menciona en sus conclusiones: (traducción libre propia)

> *"WhatsApp usa la información de la lista de contactos de Gmail para añadir contactos a lista de WhatsApp. La aplicación usa esa información para ver si uno de los contactos de Gmail tiene también una cuenta de WhatsApp y si es así, añadirlo a la cuenta de WhatsApp".*

Hizo pruebas y pudo obtener la imagen de perfil de un contacto, conociendo su número de teléfono, pero no pudo revisar el tráfico, porque se manda cifrado y no pudo descifrarlo con un certificado falso. Esta ahí todo bien, pero (Martijn, 2013) también comenta de los permisos excesivos de la aplicación para Android: como la geolocalización aproximada y precisa, y el registro de las llamadas y poder hablar directamente a un teléfono sin confirmación (aunque después se conocería que permite hacer llamadas telefónica por internet).

Un estudio europeo (Luigi Vigneri, 2015) encontró que las aplicaciones Android se conectan a sitios de rastreo de terceros, sitios maliciosos y con flujos que brincan la protección del

cortafuego, entre ellas se encontraba El navegador, Whatsapp, Messenger y Facebook, comentado en (Brinkmann, 2015)

> *"Sobre redes sociales por internet, en especial Facebook,* (Tello-Díaz, 2013) *comenta en su trabajo: implica un replanteamiento de los principios de la ética informativa relativos a la salvaguarda de la intimidad, la protección de la vida privada y el resguardo de la propia imagen. Esta investigación estudia cómo estas áreas no solo se ven afectadas por los cambios tecnológicos y la propia naturaleza de la fuente informativa, sino por la confianza y desconocimiento de los usuarios, quienes dan primacía a la comunicación por encima de la intimidad. Este fenómeno denominado «extimidad» por Jacques Lacan, se traduce como la intimidad hecha pública a través de las nuevas redes de comunicación o intimidad expuesta. En nuestro análisis expondremos los resortes a través de los cuales se quebranta nuestra privacidad en Facebook, especialmente por medio de la captación de pautas de comportamiento, el empleo de datos derivados de los perfiles, los cambios en la política de privacidad y el reconocimiento facial, avalando su transgresión con documentación derivada de investigaciones realizadas por organismos internacionales."*

(Bernhard Debatin, 2009) reseñan que hay personas que tienen preocupación por su privacidad al subir grandes cantidades de información y otras personas que escuchan eso no ponen más control a su cuenta debido a la gratificación, patrón de uso y un mecanismo psicológico del efecto de terceros, donde el uso seguro de las redes sociales necesita un cambio de actitud.

(Na Wang, 2011) Estudian sobre la ilusión de control de las aplicaciones de terceros usando información de Facebook, ante el número creciente de sitios que permiten firmarse con Facebook y la gran cantidad de aplicaciones que piden los datos, es posible que el usuario no se tan consiente de todos los lugares que extraen información de su perfil. Aunque ya existen controles en Facebook que permiten eliminar las aplicaciones que ya no usemos o no confiemos con nuestros datos.

Y ante la cada vez mayor oferta de espacios de almacenamiento en internet (la nube) y gratis, el respaldo de las fotos de los celulares en la nube, deja a los usuarios expuestos ante programas del gobierno que espían los contenidos en servidores de E.U. la NSA sobre Google y Yahoo! según

(Barton Gellman, 2013) y en México que compran software italiano de espionaje de *The Hacker Team* (Rangel, 2015).

(Iulia Ion, 2011) Menciona en su obra por medio de mi traducción libre:

> *"Los usuarios están menos preocupados sobre algunos temas, como la garantía de borrado de los datos, el país de almacenamiento y su subcontratación. Pero tienen dudas acerca de almacenar en la nube. Creen que el internet es intrínsecamente inseguro y prefieren el almacenamiento local para datos sensibles sobre el almacenamiento en la nube. Sin embargo los usuarios desean mejor seguridad y están listos para pagar por servicios que provean fuertes garantías de privacidad.*
>
> *Los participantes tienen falsas concepciones sobre los derechos y garantías de los proveedores de almacenamiento en la nube, por ejemplo, creen que el proveedor es confiable en caso de pérdida de datos, que no tienen derecho a ver o modificar sus datos y no pueden deshabilitar sus cuentas…. además de aceptar que la agencias de la ley puedan monitorear sus cuentas."*

Normalmente al usar internet dejamos huellas, que pueden y son usadas por las compañías y el gobierno. Para aprender sobre esos temas y sus cuidados están los tutoriales de la (Internet Society) donde nos explican que es la huella digital en sitios web y compras en línea, redes sociales, dispositivos móviles, administrar nuestra huella digital sus costos y beneficios.

El 28 de enero se celebra desde 2007 el Día Internacional de la Protección de Datos, o Día de la Privacidad en E.U. y Europa Según (Gonzalez, 2015). Para conocer una línea de tiempo sobre la vigilancia de EU a sus ciudadanos y al mundo revisar: https://www.eff.org/nsa-spying/timeline .

CONTRASEÑAS, ENCRIPTACIÓN

Existe dos elementos que nos van servir a mejorar la privacidad, una son las contraseñas seguras y otro la encriptación. Como recomendación no se debe poner la misma contraseña a todos los sitios, no incluir palabras de un diccionario. Combinar nemotécnicos de una frase, más números

y signos, poner las 3 últimas letras de un sitio y una palabra inventada. Y se recomienda cambiarla con frecuencia.

Según la (Web Whatsmypass, 2008) hace una listas de las 500 contraseñas más utilizadas y las 10 más comunes en inglés son: 123456, password, 12345678, 1234, pussy, 12345, dragon, qwerty, 696969, Mustang. Recomendaciones para crear contraseñas en: http://www.arturogoga.com/2009/08/28/tips-cmo-crear-contraseas-seguras-protegerlas-y-recordarlas/ .

Además otro sitio que permite crear una contraseña fuerte que permita almacenarse en un gestor de contraseñas seria: http://www.crearcontraseña.com

Microsoft ofrece un sitio con recomendaciones para crear contraseñas y para probar la fortaleza de la contraseña en:
http://www.microsoft.com/es-xl/security/online-privacy/passwords-create.aspx
https://www.microsoft.com/security/pc-security/password-checker.aspx

Recomienda Comenzar por una frase, quitarle los espacios, abreviar o escribir mal alguna palabra y agregar números con significado al final de la frase.

Adicionalmente (Microsoft Windows 7) recomienda lo siguiente para crear una frase de contraseña segura, que al ser más largas son más seguras:

- *"De 20 a 30 caracteres de longitud*
- *Es una serie de palabras que forman una frase*
- *No debe contener frases comunes de la literatura o música*
- *No debe tener su usuario, nombre real o compañía donde trabaja*
- *Es significativamente diferente de otras contraseñas y frases de contraseñas"*

Y para frases de contraseña que se pueden memorizar, pero que aún la NSA (agencia de seguridad de E.U.) no puede adivinar (Lee, 2015) nos presenta el uso de un dado y de acuerdo al

número se toma una palabra de una lista disponible en http://world.std.com/~reinhold/dicewarewordlist.pdf

Si se seleccionar una palabra de la lista hay una posibilidad entre 7,776 según el autor citado, se eleva al cuadrado con 60,466,176 posibilidades, adivinado después de 30 millones de intentos. Una frase de 5 palabras tendría 14 quintillones de intentos, un 14 y 18 ceros.

Encriptación es un anglicismo y su equivalente en español es cifrado y es una manera de codificar la información para protegerla de terceros. Cuando las claves para cifrar y descifrar son las mismas se llama criptografía simétrica y cuando son diferentes asimétrica; en esta última existe una clave privada para codificar y una pública para descifrar. Y una longitud de la clave donde a mayor tamaño, mayor seguridad y más lento se procesa. Los sistemas de clave pública se utilizan en las firmas digitales.

Según la Wikipedia las Ventajas y desventajas del cifrado asimétrico son:

- *"La mayor ventaja de la criptografía asimétrica es que la distribución de claves es más fácil y segura ya que la clave que se distribuye es la pública manteniéndose la privada para el uso exclusivo del propietario, pero este sistema tiene bastantes desventajas:*
- *Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.*
- *Las claves deben ser de mayor tamaño que las simétricas. (Generalmente son cinco o más veces de mayor tamaño que las claves simétricas)*
- *El mensaje cifrado ocupa más espacio que el original."*

La misma fuente sobre métodos de cifrado anota:

> *"Los métodos más conocidos son el DES, el Triple DES y el AES para la criptografía simétrica, y el RSA para la criptografía asimétrica"*

Debido a programas fácilmente conseguibles como menciona (Martijn, 2013) se pueden examinar el tráfico de red y si esta encriptado es más laborioso de descifrar dependiendo de la fortaleza de clave, por lo que siempre debemos revisar que las páginas de internet que pidan datos de inicio de sesión tengan el protocolo de HTTP seguro que inicia la dirección con https y

si son aplicación de mensajería e incluso de almacenamiento de archivos los datos estén encriptados para mayor seguridad.

Cabe mencionar que aunque el contenido este cifrado o encriptado todavía se puede rastrear la dirección de internet (IP), por lo cual se recomendaría el uso de Redes Privadas Virtuales o de una Red anónima como TOR.

MEDIDAS DE PRIVACIDAD DE FIREFOX, GOOGLE, FACEBOOK, WHATSAPP

Se recomienda fuertemente revisar el sitio de *StaySafeonline.org* patrocinado por (National Cyber Security Alliance). Donde ofrece recomendaciones para revisar su configuración de privacidad en sitios de Comercio electrónico, correo, servicios de geolocalización, música, compartir fotos, buscadores, redes sociales, videos, modo incógnito de los navegadores y más.

Además Ofrece recursos para estar seguros en línea, su enseñanza, negocios seguros e involucrarse en el tema.

Otra fuente de información recomendada es el informe de la (Electronic Frontier Foundation) acerca de la posición de las compañías sobre su transparencia en la protección de datos de las solicitudes del gobierno, Con criterios de seguir las mejores prácticas de la industria (el único que no cumple es Whatsapp), informar a los usuarios sobre las solicitudes de datos de gobierno (incumplen Amazon, Google, Slack, twitter, Whatsapp etc.), políticas de informar de retención de datos (incumplen Amazon, google , Microsoft, Whatsapp), informar solicitudes de eliminación de contenido (mal por Facebook, linkedin, Microsoft) y política pública pro-usuario contra las puertas traseras (incumplen: AT&T, Reddit,Verizon).

Donde los mejor portados (cumplen con todos los apartados) son, Adobe, Apple, Dropbox, Sonic, Wickr, Wikimedia, Wordpress, Yahoo!. Y la peor Whatsapp que solo cumple una y fue cuando la adquirió Facebook.

Firefox

El sitio de (Mozilla Firefox) menciona las medidas para proteger la privacidad a través de configuraciones para no rastrear, navegación privada, el botón olvidar cierto tiempo del historial. Mejora la seguridad a través de conexiones seguras, protección de clase mundial contra malware y *phishing* y actualizaciones de seguridad automáticas.

Además a través del sitio mozilla.org/es-MX/privacy/tips/ ofrece un "master" en privacidad en cuatro sencillos pasos: pregunta, aprende, actúa y discute. ¿Qué importancia le concede a la privacidad?, usar el complemento *lightbeam* para arrojar luz sobre quién te observa, usar las características de no ser rastreado, botón olvidar, *duckduckgo* y los complementos de privacidad. Además de recomendar el sitio de *staysafeonline.org* para activar la seguridad sobre la marcha, protegerse en las redes sociales y comprobar los ajustes de privacidad. Y nos pregunta ¿hasta qué punto nos preocupa quién tiene acceso a nuestros datos en la red (empresas de publicidad, corporaciones, gobiernos, etc.)?

Aun así, la compañía quiere hacerse llegar recursos de publicidad, basado en los ámbitos de navegación y lo hará a través de las miniaturas mejoradas que podrán ofrecer contenido patrocinado, específicamente etiquetado y se podrán deshabilitar desde la Navegación, como comenta la ayuda del Navegador y funciona desde fines de mayo del 2015.

Google

Hace 20 años, se usaban los marcadores para recordar páginas interesantes, luego usamos el historial de los navegadores. Pero ahora siempre que iniciamos sesión quedan guardadas nuestras búsquedas y si no solo la dirección de internet y la búsqueda. Si entramos con nuestra cuenta de Google podemos revisar nuestro archivo de búsqueda que ellos dicen solo podemos ver nosotros en: https://history.google.com/history/

Pero no solo eso tenemos información de los dispositivos móviles desde los que realizamos búsquedas, historial de ubicaciones, domicilio de la casa y el trabajo, historial de reproducciones de YouTube. Y a través de la misma, en la parte superior derecha un icono de 3 puntos, en configuración se puede descargar las búsquedas, se puede borrar direcciones que no queramos tener guardadas y desactivar el historial de aplicaciones. Al hacerlo esos contenidos dejan de

estar asociados a su cuenta de Google, pero puede almacenar la actividad por separado para evitar el spam y el uso inadecuado, así como para mejorar sus servicios, según (Google).

Cabe mencionar que los anuncios que ofrece en el correo electrónico Gmail, se basa en el contenido de los mismos y es su fuente principal de ingreso, por lo que es recomendable cifrar los correos o cambiar de servidor a otro que no sea Microsoft, Yahoo! o Apple. Se recomienda Tutanota, que aunque también tiene una versión comercial, tiene la opción de cifrado de punto a punto y aplicaciones móviles para Android y iOS. Una alternativa prometedora es bitmessage (para computadoras de escritorio), de los creadores de bitcoin que manda encriptado los mensajes a través de una red Peer to peer (punto a punto) anónima, recomendándose tener un ID realmente generado al azar. Una opción libre cifrada de cero conocimiento es la alemana Lavaboom, donde es por invitación.

En vez de su servicio de archivos se puede usar Copy que da 15 Gb gratis, tiene visor de documentos de Word, es cifrado y permite subir fotos del celular, y cuenta con aplicaciones móviles para Android y iOS,. No es software libre como si lo es**:** owncloud y peerio**,** este último encripta los archivos con una frase contraseña y está en proceso de crear sus aplicaciones móviles, donde permite que los archivos se pueda autodestruir de forma remota.

Para un equivalente libre a los documentos de Google en Drive: para colaborar tenemos Kune (web, español) o el propietario Slash, (Windows, móvil) o Hipchat (escritorio y móvil). Una opción libre en línea con aplicaciones empresariales es Onlyoffice.com, se puede descargar gratis e instalar en el servidor, o si es una escuela u organización sin fines de lucro, piden un banner en su página principal, para usar gratis la versión en línea (disponible en español).

También se encuentra los programas de Etherpad, para crear documentos colaborativos en tiempo real, ethercalc: un servidor de hojas de cálculo multiusuario; etherdraw, herramienta de dibujo y protectedText encripta y desencripta en el navegador de forma que nunca se manda la contraseña al servidor. Y dudle, para encuestas seguras hospedadas en línea. En escritorio tenemos el Libreoffice y para Android el Andropen office. Prezi (privativo) es una forma moderna de crear presentaciones, pero la compañía tiene oficinas en San Francisco, E.U. Aunque dice que usa SSL para la transmisión de los datos, no ha sido auditada por especialistas de seguridad. Calliga Suite es una suite más completa en Linux y se puede simular en Windows y Mac OS X a través de aplicaciones que ejecutan el escritorio de KDE.

Para el hospedaje de imágenes con encriptación en el navegador con AES de 256 bit se encuentra **https://img.bi/** .

GNU MediaGoblin, es una plataforma web de software libre para alojar y compartir multimedia digital. A parte de poderlo instalar en un servidor propio, se pueden usar los siguientes: https://goblinrefuge.com/mediagoblin/ (inglés), https://mediagoblin.pixelminers.net/ (español) requiere crear una cuenta en Mozilla Persona (que se utiliza en otros sitios), pero hay más en https://wiki.mediagoblin.org/Live_instances . Y Libre.fm, es el "spotify" de música libre.

Para una discusión más detallada para sustituir la mayoría de los servicios de Google se recomienda el siguiente web http://www.thelastblog.net/se-puede-vivir-sin-google-os-proponemos-alternativas-para-sus-mas-populares-servicios/

Facebook

El sitio de privacidad de (Facebook) ofrece información acerca de lo que los demás ven de uno, como interactúan lo demás, lo que uno ve, como proteger la cuenta y la política de datos.

En la (Ayuda de Facebook) aparecen los ajustes de privacidad de perfil y biografía, ajuste de lo que pueden ver los demás: el control de quien puede ver el contenido del perfil, las publicaciones de los amigos en la biografía, publicaciones anteriores y como se ve el perfil a otros. En otras herramientas y opciones de configuración: información del perfil, revisión de la biografía, quien puede ver el correo electrónico del perfil, quien puede ver la sección de amigos, como se controla que publiquen en el perfil, donde se pueden ver las publicaciones pendientes de la biografía.

En la parte superior derecha del servicio web de Facebook aparece un icono de un candado como acceso directo de la privacidad, donde aparecen las opciones de configuración de privacidad, ¿quién puede ver las cosas?, ¿Quién me puede contactar?, y ¿cómo evito que alguien me moleste?. En la comprobación aparecen las opciones de las publicaciones (su alcance), las aplicaciones que se usa (¿quién las ve?) y los datos del perfil (¿quién las ve?, si es público, los amigos, solo yo o algún grupo de mis amigos.

Lo anterior da una idea de más seguridad pero las condiciones de uso de Facebook son muy generosas, de acuerdo con (Velasco, 2014) estas son algunas de las más interesantes:

* Se auto-atribuye una licencia de uso mientras seamos usuarios del servicio y, por tanto, puede usar nuestros contenidos o los que generemos en aplicaciones conectadas con Facebook.

* Si eliminamos un contenido, la compañía guarda copias de seguridad y los retiene durante un tiempo. Aún eliminando la cuenta, tiene un respaldo, guarda los me gusta y los contenidos públicos.

* Que una aplicación acceda a nuestros datos, según Facebook depende de nosotros.

* Por el hecho de usar Facebook, los usuarios nos convertimos en "producto" de los anunciantes de la plataforma, pueden usar nuestro contenido en campañas publicitarias, con implicación obligatoria ante nuestros amigos y sin paga.

* Los datos se almacenan en E.U. y rigen sus leyes. Las condiciones del servicio pueden cambiar cuando ellos deseen.

*Para poderse registrar deben tener 13 años y anotar los datos reales. Puede quitar contenidos si considera que se violan sus políticas.

* La cuenta puede darse de baja o desactivarse de manera temporal tanto por nosotros mismos como por Facebook.

* Facebook no garantiza que su plataforma sea segura, no ofrece garantías de la disponibilidad del servicio y si no cumple alguna de sus cláusulas no pasa nada. Y remata con "Nos reservamos todos los derechos que no te hayamos concedido de forma expresa".

Además con la actualización de diciembre del 2014, está solicitando a los usuarios su consentimiento para rastrear la ubicación. Y usar el GPS y/o Wifi y permitir que los amigos puedan seguir sus movimientos.

Whatsapp

(jlacort, 2013) resume las condiciones que se aceptaron al usar Whatsapp:

- *WhatsApp sólo puede ser usado por mayores de 16 años.*
- *WhatsApp puede cambiar las condiciones cuando quiera, el usuario es responsable de revisarlas periódicamente para ver si hay cambios y decidir si continúa utilizando el servicio o no.*
- *WhatsApp no garantiza la confidencialidad de conversaciones y contenidos intercambiados en su servicio.*
- *WhatsApp no borra conversaciones, sólo las oculta.*
- *A WhatsApp no le enviamos sólo nuestro teléfono, sino nuestra agenda completa.*
- *No sólo recibe los números de nuestra agenda, sino la información completa de cada tarjeta de contacto: nombre y apellidos, correo electrónico asociado, y si somos detallistas y rellenamos todos los campos posibles, hasta cumpleaños, foto o dirección física, entre otros.*
- *Para que esos números estén ahí, WhatsApp da por sentado que esas personas nos han dado su permiso.*
- *WhatsApp deja claro que el uso comercial está prohibido, quedando limitado al uso estrictamente personal.*
- *Si se puede enviar contenido para adultos pero sí se debe indicarlo directamente de forma previa a ese contenido.*
- *WhatsApp se lava las manos respecto al contenido que enviemos mediante él.*
- *Queda prohibido utilizar parte de WhatsApp para crear servicios clónicos o que emulen la aplicación.*
- *WhatsApp obliga a informarle si nos roban o perdemos nuestro terminal.*
- *Queda prohibido el uso de bots que envíen mensajes masivos.*
- *No podemos enviar contenido del cual no seamos propietarios o tengamos el permiso de su autor.*
- *Si violamos las condiciones en repetidas ocasiones, WhatsApp puede eliminarlos del servicio. Curiosamente, para determinar si hemos incurrido en esto durante las*

ocasiones suficientes, WhatsApp se acogerá al criterio de sus authorized WhatsApp employees, agents, subagents, superagents or superheros.

- *Cualquier incidente que nos ocurra con WhatsApp tiene un plazo de un año para denunciarse.*

El 7 de octubre del 2014, Facebook compro a Whatsapp y sus condiciones más actuales se encuentran en: https://www.whatsapp.com/legal/#Privacy . Donde indica que no se han cambiado los términos desde julio del 2012.

El análisis de (Bölükbas, 2014) menciona los pros y contras de esa herramienta:

Ampliamente difundido, disponible para Android, iOS, BlackBerry, Windows phone, utilizando una versión personalizad del Protocolo de Presencia y Mensajería Extendida (XMPP). Sin embargo:

- Tiene un débil algoritmo de encriptación llamado "RC4 stream chiper"
- Sube el directorio de contactos a sus servidores
- No encripta la base de datos de manera local.
- Usa la misma clave HMAC en ambas direcciones
- Es código cerrado, software privativo.
- No es compatible con Tor y servidores de Proxy
- No tiene encriptación de punto a punto, ni fuera de la grabación (OTR)
- No apoya el secreto de privacidad hacia adelante.
- No tiene charlas anónimas.
- No es compatible con servidores XMPP de terceros.

En vez de usar Whatsapp se puede usar Wickr (privativo) Telegram (cliente. Software libre, servidor: propietario), pero disponible para los dispositivos móviles, en computadoras de escritorio hay varias opciones libres como Bitmessage**,** pidgin y otras.

Pero lo mínimo que debería de revisarse en Whatsapp sería de acuerdo a (Hérnandez, 2015): no guardar las fotos automáticamente (en Telegram tenemos que decirlo específicamente por cada foto), desactivar las notificaciones del Whatsapp sobre todo en iPhone en la pantalla de bloqueo, desactivar los tonos indiscretos que tiene la aplicación, filtrar la foto de perfil y estado a solo los

contactos o a Nadie y cerrar la sesión de WhatsApp web. También se puede ocultar la última conexión en los ajustes de privacidad y en ese caso tampoco conocerás esa información en tus contactos.

Una recomendación adicional, respaldar los mensajes de las conversaciones más largas y las más importantes mandándolo a un correo seguro y después limpiar el chat. También hay la opción de archivar todas las conversaciones (reversible).

Conclusión

El propósito de este artículo es tomar conciencia de la importancia de la privacidad, y el cambio de hábitos, desde revisar los ajustes de privacidad de los servicios que usamos, usar contraseñas fuertes y encriptación a instalar complementos para privacidad, soluciones de software libres y ser promotores de la privacidad en Internet.

Puede que de principio sospecháramos algo, me están dado estos servicios gratis y son amigables, y se pagan por publicidad, pero esa publicidad sale de espiar mis datos y antes de depender más de estos servicios, tomar conciencia de la huella digital y pensar en el futuro, así que si no lo hacemos en la vida real, en público, no deberíamos hacerlo en línea y si queremos proteger nuestros pensamientos tenemos herramientas para protegernos.

Los ataques a la privacidad continúan, ahora se revela que los gobiernos de E.U. e Inglaterra ya están espiando las comunicaciones encriptadas según (Greenwald, 2013), además de distribuir malware para infectar computadoras antes de encriptar, y tienen técnicas para atacar las VPN, según artículos citados por (Electronic Frontier Foundation) por ello los usuarios criminales seguirán siendo vigilados. Pero sigue siendo importante el uso de contraseñas fuertes y estar al corriente de lo que los auditores de seguridad ofrecen sobre los sitios y servicios en línea.

Lo más preocupante, es que los teléfonos celulares inteligentes están haciendo más fácil espiar a sus dueños, especialmente los Android que son los más económicos, y la mayoría de la población no sospecha, ni desconfía de la información que almacena, con muchos datos privados. Espero que los lectores de este trabajo puedan difundir el tema y ser promotores del mismo, por el bien suyo, de su comunidad, país y de todo el ciberespacio.

Bibliografía

Amaro, L. R. (2013). Espacio, tiempo y privacidad en la comunicación móvil. *Realitas, Revista de ciencias sociales, humanas y artes*, 32-36.

Ayuda de Facebook. (s.f.). *Privacidad del perfil y la biografía*. Recuperado el 5 de Agosto de 2015, de https://www.facebook.com/help/393920637330807/

Barton Gellman, A. S. (30 de octubre de 2013). *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say.* Recuperado el 2 de mayo de 2015, de The Whashington Post: https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Bernhard Debatin, J. P.-K. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, 83-108.

Bölükbas, C. (3 de Abril de 2014). *Candan Bölükbas Technology Blog.* Recuperado el 4 de Agosto de 2015, de Security Evaluation for Instant Message (IM) Apps: http://blog.candan.expert/2014/04/security-evaluation-for-instant-message_3.html

Bonifaz, R. (4 de Diciembre de 2013). *PillKu amantes de la libertad*. Recuperado el 15 de julio de 2015, de La vigilancia en internet y el programa PRISM: http://www.pillku.com/article/la-vigilancia-en-internet-y-el-programa-prism/

Bonifaz, R. (25 de julio de 2015). *Campus Party México*. Recuperado el 25 de julio de 2015, de Privacidad en Internet: https://www.youtube.com/watch?v=_9XEy4hyuUQ&utm_source=twitterfeed&utm_medium=twitter

Brinkmann, M. (3 de mayo de 2015). *NoSuchApp for Android highlights apps secretly connecting to tracking sites.* Recuperado el 6 de mayo de 2015, de Ghacks.net: http://www.ghacks.net/2015/05/03/nosuchapp-for-android-highlights-apps-secretly-connecting-to-tracking-sites/

Electronic Frontier Foundation . (s.f.). *Electronic Frontier Foundation* . Recuperado el 5 de agosto de 2015, de https://www.eff.org/who-has-your-back-government-data-requests-2015

Facebook. (s.f.). *bases para proteger tu privacidad*. Recuperado el 5 de agosto de 2015, de https://www.facebook.com/about/basics/

FM, Y. (26 de enero de 2015). *GenBeta*. Recuperado el 2 de Mayo de 2015, de ¿Se puede vivir sin Google? Os proponemos alternativas para sus más populares servicios: http://www.thelastblog.net/se-puede-vivir-sin-google-os-proponemos-alternativas-para-sus-mas-populares-servicios/

GenBeta. (s.f.). *Crear Contraseñas seguras.* Recuperado el 5 de Agosto de 2015, de http://www.genbeta.com/tag/especial-contrasenas-seguras

Gonzalez, G. (28 de enero de 2015). *hipertextual*. Recuperado el 5 de Agosto de 2015, de Hoy se celebra el Día de la Privacidad, puedes celebrarlo aprendiendo a proteger tus datos: http://hipertextual.com/2015/01/dia-de-la-privacidad

Google. (s.f.). *Ayuda de Búsquedas web*. Recuperado el 5 de agosto de 2015, de Eliminar las búsquedas y la actividad de navegación: https://support.google.com/websearch/answer/465?hl=es

Greenwald, G. (5 de septiembre de 2013). *The Guardian.com*. Recuperado el 5 de agosto de 2015, de Revealed: how US and UK spy agencies defeat internet privacy and security: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Greenward, G. (octubre de 2014). *Why privacy matters?* Recuperado el 14 de Julio de 2015, de TED talks: http://www.ted.com/talks/glenn_greenwald_why_privacy_matters

Hérnandez, K. (19 de marzo de 2015). *CNN expansión*. Recuperado el 5 de Agosto de 2015, de 5 tips para mantener tu privacidad en WhatsApp: http://www.cnnexpansion.com/tecnologia/2015/03/18/5-tips-para-mantener-tu-privacidad-en-whatsapp

hotspotshield. (s.f.). *hotspotshield by anchorfree.* Recuperado el 5 de agosto de 2015, de Tor vs VPN: http://www.hotspotshield.com/learn/tor-vs-vpn

Internet Society. (s.f.). *Internet Society.* Recuperado el 08 de agosto de 2015, de Tu huella digital: http://www.internetsociety.org/es/tu-huella-digital

Iulia Ion, N. S. (2011). Home is safer than the cloud!: privacy concerns for consumer cloud storage. *Proceeding SOUPS '11 Proceedings of the Seventh Symposium on Usable Privacy and Security* (págs. 1-20). New York, NY, USA: ACM.

jlacort. (13 de diciembre de 2013). *Hipertextual.* Recuperado el 22 de Agosto de 2015, de Resumen de las condiciones de WhatsApp: esto es lo que aceptaste sin saberlo: http://hipertextual.com/archivo/2013/12/condiciones-whatsapp/

Julian, G. (24 de julio de 2014). *Genbeta.* Recuperado el 4 de Agosto de 2015, de Canvas fingerprinting: cómo evitar ser rastreado y monitorizado por todo Internet: http://www.genbeta.com/actualidad/canvas-fingerprinting-como-evitar-ser-rastreado-y-monitorizado-por-todo-internet

Lee, M. (26 de marzo de 2015). *PASSPHRASES THAT YOU CAN MEMORIZE — BUT THAT EVEN THE NSA CAN'T GUESS.* Recuperado el 21 de julio de 2015, de First Look: https://firstlook.org/theintercept/2015/03/26/passphrases-can-memorize-attackers-cant-guess/

Luigi Vigneri, J. C. (27 de abril de 2015). *Taming the Android AppStore: Lightweight Characterization of Android Applications.* Recuperado el 6 de Mayo de 2015, de Arvxiv.org: http://arxiv.org/pdf/1504.06093v2.pdf

Martijn, T. (3 de Julio de 2013). *Whatsapp and Privacy.* Recuperado el 18 de Mayo de 2015, de Computing Science Department - Radboud University Nijmegen: http://www.cs.ru.nl/bachelorscripties/2013/Martijn_Terpstra___0814962___WhatsApp_and_privacy.pdf

Microsoft Windows 7. (s.f.). *Tips for creating strong passwords and passphrases.* Recuperado el 21 de Julio de 2015, de Microsoft: http://windows.microsoft.com/en-us/windows7/tips-for-creating-strong-passwords-and-passphrases

Mozilla Firefox. (s.f.). *Ayuda de Mozilla Firefox.* Recuperado el 4 de agosto de 2015, de Navegación privada: navega en la Web sin guardar información sobre los sitios que visitas: https://support.mozilla.org/es/kb/navegacion-privada-navega-en-la-web-sin-guardar-in?redirectlocale=en-US&redirectslug=private-browsing-browse-web-without-saving-info

Mozilla Firefox. (s.f.). *De confianza*. Recuperado el 5 de Agosto de 2015, de https://www.mozilla.org/es-MX/firefox/desktop/trust/

Na Wang, H. X. (2011). Third-party apps on Facebook: privacy and the illusion of control. *Proceeding CHIMIT '11 Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology* (págs. 1-10). New York, NY, USA: ACM.

National Cyber Security Alliance. (s.f.). *Staysafeonline.org.* Recuperado el 8 de agosto de 2015, de Check Your Privacy Settings: https://www.staysafeonline.org/data-privacy-day/check-your-privacy-settings/

Rangel, A. (7 de Julio de 2015). *México, el principal cliente de una empresa que vende software para espiar.* Recuperado el 20 de julio de 2015, de Animal Politico: http://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/

Tactical Technology Colletive & Frontline defenders. (s.f.). *Bienvenido a la Caja de Herramientas de Seguridad.* Recuperado el 6 de Agosto de 2015, de herramientas y teacticas para una seguridad digital: https://info.securityinabox.org/es

Tello-Díaz, L. (2013). Intimidad y "extimidad" en las redes sociales. Las demarcaciones éticas de Facebook. *Revista Comunicar*, 205-213.

Thomas, P. L. (22 de septiembre de 2010). *EDUCASE REVIEW.* Recuperado el 18 de Mayo de 2015, de http://www.educause.edu/ero/article/death-digital-dropbox-rethinking-student-privacy-and-public-performance

Velasco, J. (6 de febero de 2014). *Hipertextual.* Recuperado el 5 de Agosto de 2015, de Condiciones de Facebook: todo lo que aceptase sin leer, explicado de forma clara: http://hipertextual.com/2014/02/condiciones-facebook

Web Whatsmypass. (30 de Noviembre de 2008). *The Top 500 Worst Passwords of All Time.* Recuperado el 21 de Julio de 2015, de Whatsmypass: http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time

Zhong, P. (s.f.). *PRISM BREAK*. Recuperado el 29 de julio de 2015, de opta por salir de los programas globales de vigilancia de datos de PRISM, Xkeyscore y Tempora: https://prism-break.org/es/