Guía Paso a Paso

Esta Guía Paso a Paso está diseñada para explicar los temas que debes entender con el fin de salvaguardar tu propia seguridad digital. Esta busca identificar y describir los riesgos que enfrentas y ayudarte a tomar decisiones informadas de cómo reducir, de la mejor manera, dichos riesgos. En este extremo, responde a ocho preguntas generales relacionadas a seguridad básica, protección de datos y privacidad de las comunicaciones.

Al inicio de cada capítulo, encontrarás un contexto poblado de personajes ficticios que reaparecerán en breves diálogos a lo largo del capítulo con el fin de ilustrarte sobre ciertos aspectos y respuestas a preguntas comunes. También encontrarás una corta lista de lecciones especificas que pueden ser aprendidas a partir de la lectura del capítulo. Es una buena idea darle un vistazo a esta lista antes de que empieces a leer. A medida que te desplazas en el capitulo, encontraras varios términos técnicos que se enlazan con definiciones en un glosario que se halla al final de la guía. También encontraras referencias al programa específico tratado en el paquete de las Guías Prácticas.

Cualquier capitulo o guía independiente en este paquete puede leerse individualmente, darle formato en tu navegador para una fácil impresión, o compartirlo electrónicamente. Sin embargo, aprovecharás de mejor manera la Caja de Seguridad si sigues los enlaces pertinentes y las referencias que están esparcidas a lo largo de la guía y de las guías de los programas. Si tienes una copia física de la Guía Paso a Paso, debes mantenerla frente a ti mientras trabajas con las Guías Prácticas. También debes recordar el finalizar la lectura del capitulo de la Guía Paso a Paso que cubre una herramienta específica antes de confiar en dicha herramienta para que proteja tu seguridad digital.

En la medida de lo posible, debes leer los capítulos de la Guía Paso a Paso en orden. La seguridad es un proceso, y no es coherente intentar defenderte de una amenaza avanzada a la privacidad de tus comunicaciones, por ejemplo, si no has garantizado que tu computadora está libre de virus y de otros software malintencionados (malware). En muchos casos, esto puede parecerse a cerrar tu puerta una vez que el ladrón está ya en tu casa. Esto no quiere decir que alguno de los ocho temas sea más importante que cualquier otro, sino que simplemente los últimos capítulos hacen algunas suposiciones sobre lo que ya sabes y sobre el estado de la computadora en la cual instalarás el programa.

Claro que existen muchas buenas razones por las que tú quisieras recorrer estos capítulos sin secuencia. Puede que necesites consejos de cómo crear un respaldo a tus archivos más importantes antes de empezar a instalar las herramientas descritas en la primera Guía Práctica. Puede ser que afrontes una amenaza urgente a tu privacidad que justifica que aprendas como proteger tu información sensible en tu computadora, lo cual esta cubierto en el *Capítulo 4*, lo más rápido posible. Talvez estás trabajando en un café Internet, en una computadora cuya seguridad no es tu responsabilidad y desde la cual no pretendes acceder a alguna información sensible. Si deseas utilizar esta computadora para visitar un sitio web que esta bloqueado en tu país, no existe nada que te impida saltar hasta el *Capítulo 8. Mantenerse en el anonimato y evadir la censura en Internet*.

1. Proteger tu computadora de software malicioso (malware) y piratas informáticos (hackers)

Sin importar cuales sean tus más amplios objetivos, el mantener tu computadora libre de problemas es un primer paso indispensable en la senda de una mejor seguridad. Por ello, antes de empezar a preocuparte demasiado - por ejemplo, acerca de contraseñas sólidas - comunicación privada y borrado seguro, necesitas garantizar que tu computadora no sea vulnerable a los *piratas informáticos (hackers)* [1] o no esté plagada de *software malicioso (malware)* [2], tales como virus y software espía (spyware). De lo contrario, es imposible garantizar la efectividad de cualquier otra precaución de seguridad que pudieras tomar. Después de todo, no tiene sentido cerrar la puerta si el ladrón ya se encuentra en nuestras escaleras, y tampoco es bueno buscar en las escaleras si dejas la puerta completamente abierta.

De la misma manera, este capítulo explica como mantener tu software y utilizar herramientas como el *Avast* [3], *Spybot* [4] y *Comodo Firewall* [5] para proteger tu computadora de peligros permanentes de infección de *software malicioso (malware)* [2] y ataques de *piratas informáticos (hackers)* [1] . Aunque las herramientas recomendadas en este capítulo son para Windows - que es el sistema operativo más vulnerable a estas amenazas - los usuarios de *GNU/Linux* [6] y Apple OS X también se hallan en riesgo y deben seguir las tácticas referidas a continuación.

Contexto

Assani es un activista de derechos humanos en un país africano francófono. Sus dos hijos adolescentes, Salima y Muhindo, se han ofrecido a ayudarle con algo de trabajo informático de rutina que le solicitaron a él. Después de ver el estado de su computadora, ellos se han ofrecido a enseñarle lo fundamental en cuanto a mantenerla libre de problemas

y funcionando plenamente. A Assani también le entusiasma la idea de utilizar Software Libre y de Código Abierto (FOSS) , pero no está seguro si ello será más o menos seguro, de modo que también les pide su consejo.

¿Qué aprenderás en este capítulo?

- Unas cuantas amenazas específicas que plantea el *software malicioso (malware)* [2] a la privacidad e integridad de tu información, la estabilidad de tu computadora y la confiabilidad de otras herramientas de seguridad
- Cómo puedes utilizar varias herramientas recomendadas para ayudar a protegerte de estas amenazas
- Cómo mantener tu computadora segura actualizando tu software frecuentemente
- Porqué debes utilizar herramientas de *software gratuito (freeware)* [7], para evitar los peligros asociados con licencias expiradas o software pirata, y populares herramientas de *Software Libre y de Código Abierto (FOSS)* [8], cuando sea posible para mejorar tu seguridad

Virus

Existen muchas maneras distintas de clasificar los virus, y cada una de estas viene acompañada de su propia colección de categorías con nombres pintorescos. Gusanos, macrovirus, troyanos y puertas traseras (backdoors) son algunos de los ejemplos más conocidos. Muchos de estos virus se extienden en Internet, utilizando el correo electrónico, páginas web maliciosas u otros medios para infectar computadoras no protegidas. Otros se propagan a través de medios extraíbles, particularmente a través de dispositivos USB y de discos duros externos que permiten a los usuarios escribir y leer información. Los virus pueden destruir, dañar o infectar la información en tu computadora, incluyendo datos en discos externos. Estos también pueden tomar control de tu computadora y utilizarla para atacar a otras. Afortunadamente existen muchas herramientas antivirus que puedes utilizar para protegerte y proteger a aquellos con los cuales intercambias información digital.

Software Antivirus

Existe un excelente programa antivirus que además es *software gratuito (freeware)* [9] para Windows llamado *Avast* [10], el cual es fácil de utilizar, se actualiza de manera regular y es respetado por los expertos en programas antivirus. Este requiere que te registres una vez cada 14 meses, pero el registro, las actualizaciones y el programa son gratuitos.

Parte Práctica: Empieza con la *Guía del Avast* [11]

Clam Win [12] es una alternativa de *Software Libre y de Código Abierto (FOSS)* [13] al *Avast* [10] y de varios conocidos programas comerciales antivirus. Aunque carece de ciertas características que son importantes para un programa antivirus básico, Clam Win tiene la ventaja que puede ser ejecutado desde una memoria extraíble USB con el fin de escanear una computadora en la cual no se te permite instalar software. Esto es extremadamente útil cuando no tienes otra opción más que utilizar una computadora pública o los cafés Internet para realizar trabajo sensible.

Consejos para utilizar software antivirus de manera eficaz

- No ejecutes dos programas antivirus al mismo tiempo, pues ello podría causar que tu computadora funcione de manera extremadamente lenta o que se cuelgue. Desinstala uno antes de instalar otro.
- Asegúrate que tu programa antivirus te permita recibir actualizaciones. Como muchas de las herramientas comerciales que vienen preinstaladas en las computadoras nuevas, en algún punto se debe proceder a registrarlas (y pagar por ellas) o estas dejarán de recibir actualizaciones. Todo el software que se recomienda aquí permite actualizaciones libres de cargo.
- Cerciórate que tu software antivirus se actualice automáticamente de manera regular. Los nuevos virus se crean y propagán a diario, y tu computadora pronto se verá vulnerable si no estás al tanto de nuevas definiciones de virus. *Avast* [10]automáticamente buscará actualizaciones cuando te conectes a la Internet.
- Permite, que tu software antivirus tenga 'siempre activa' su opción de detección de virus, si cuenta con esta. Es posible que diferentes aplicaciones usen distintos nombres para esta opción pero la mayoría de ellas ofrece una opción como esta. Puede llamarse 'Protección en Tiempo Real,' 'Protección Residente,' o de alguna otra manera similar. Dirígete a la **sección 3.2.1** [14] de la **Guía del Avast** [11] para obtener detalles acerca de la herramienta de 'Escáner por Acceso.'
- Escanea regularmente todos los archivos de tu computadora. No tienes que hacer esto a diario — especialmente si tu software antivirus tiene una opción 'siempre activo', como se describe líneas arriba — pero debes hacerlo de

tiempo en tiempo. ¿Cuan a menudo?, dependerá de las circunstancias. ¿Has conectado, recientemente, tu computadora a una red desconocida? ¿Con quien has estado compartiendo tu memoria extraíble USB? ¿Recibes frecuentemente documentos adjuntos extraños con tu correo electrónico? ¿Alguien en tu casa u oficina ha tenido problemas de virus recientemente? Para mayor información de cuál es la mejor manera de escanear archivos, dirígete a la sección de la **Guía del Avast** [11].

Evitar una infección viral

- Se extremadamente cuidadoso cuando abras archivos adjuntos en tu correo electrónico. Es mejor evitar abrir cualquier archivo adjunto recibido de una fuente desconocida. Si necesitas hacerlo, debes primero guardar el archivo adjunto en una carpeta en tu computadora, luego abrir la aplicación pertinente (tal como Microsoft Word o Adobe Acrobat). Es menos probable que contraigas el virus, si utilizas el menú de Archivo del programa para abrir el archivo adjunto en forma manual, en vez de pulsar dos veces sobre el archivo o permitir que tu programa de correo electrónico lo abra automáticamente.
- Considera los posibles riesgos antes de insertar medios extraíbles, tales como CDs, DVDs y memorias extraíbles USB, en tu computadora. Primero debes verificar que tu programa antivirus tenga las últimas actualizaciones y que su escáner esta ejecutándose. También es una buena idea deshabilitar la opción 'Reproducción Automática' de tu sistema operativo, que puede ser utilizada por los virus para infectar tu computadora. Con el Windows XP, esto puede hacerse dirigiéndote a **Mi PC**, pulsando el botón derecho del ratón sobre tu unidad de CD o DVD, seleccionando **Propiedades** y pulsando sobre la pestaña **Reproducción Automática**. Para cada tipo de contenido, selecciona las opciones, **No realizar ninguna acción** o **Pregúntame siempre que elija una acción** luego pulsa **Aceptar**.
- Puedes también ayudar a evitar algunas infecciones virales cambiándote a un *Software Libre y de Código Abierto (FOSS)* [13], el cual es a menudo más seguro, y a los cuales los creadores de virus son menos propensos a atacar.

Assani: Tengo un limpiador de virus y lo ejecuto regularmente, por tanto creo que mi computadora no tiene problemas, ¿Correcto?

Salima: En realidad, el tener simplemente un software antivirus no es suficiente. También necesitas proteger tu computadora de software espía (spyware) y piratas informáticos (hackers), de modo que tendrás que instalar y ejecutar un par de herramientas más.

Software Espía (Spyware)

El software espía (spyware) es una clase de *software malicioso (malware)* [2] que puede rastrear el trabajo que haces, tanto en tu computadora como en la Internet, y enviar dicha información a alguien que no debe tener acceso a ella. Estos programas pueden registrar, entre otras cosas, las palabras que digitas en tu teclado, los movimientos de tu ratón, las páginas que visitas y los programas que ejecutas. Como resultado de ello, pueden socavar la seguridad de tu computadora y revelar información confidencial sobre ti, tus actividades y tus contactos. Las computadoras se infectan con software espía (spyware) en prácticamente la misma forma en la que contraen virus, por tanto muchas de las sugerencias realizadas anteriormente son también útiles cuando nos defendemos de esta segunda clase de software malicioso (malware). Debido a que las páginas web maliciosas son la mayor fuente de infecciones de software espía (spyware), debes prestar mayor atención a los sitios web que visitas y asegurarte que las opciones de tu navegador sean seguras.

Assani: Todo eso me suena como algo salido de una película de espías. ¿Mi computadora está en verdad "infectada con software espía (spyware)?"

Muhindo: Lo creas o no, esto es muy común. Si aquellos programas que descargaste de la Internet no te han infectado, existe una buena posibilidad de que por lo menos una de las páginas que has visitado lo haya hecho. El hecho de que utilices Windows y el Internet Explorer lo hace aun más probable. Si nunca has escaneado tu computadora en busca de software espía (spyware), te apuesto a que te sorprenderás de cuantos están instalados en ella.

Software contra Software espía (spyware)

Puedes utilizar herramientas contra software espía (spyware) para proteger tu computadora de este tipo de amenazas. El *Spybot* [4] es uno de esos programas, y hace un buen trabajo identificando y eliminando ciertos tipos de *software malicioso (malware)* [2] que los programas antivirus simplemente ignoran. Sin embargo, de la misma manera que con un programa antivirus, es extremadamente importante que actualices las definiciones de software malicioso (malware) del Spybot y que ejecutes escaneados regulares.

Parte Práctica: Empieza con la Guía del Spybot [15]

Evitar infección de software espía (spyware)

- Mantente alerta cuando navegues en sitios web. Cuídate de las ventanas de navegador que aparecen automáticamente, y léelas con cuidado en vez de pulsar simplemente Si o Aceptar. En caso de duda, debes cerrar las 'ventanas emergentes' pulsando la X en la esquina superior derecha, en vez de pulsar sobre Cancelar. Esto puede ayudarte a evitar que las páginas web te engañen instalando *software malicioso (malware)* [2] en tu computadora.
- Mejora la seguridad de tu navegador Web evitando que ejecute automáticamente potenciales programas peligrosos que a veces están contenidos dentro de las páginas web que visitas. Si utilizas Mozilla *Firefox* [16], puedes instalar el complemento *NoScript* [17], como se describe en la **sección 4** [18] de la **Guía del Firefox** [19].
- Nunca aceptes ni ejecutes este tipo de contenido si vienes de un sitio web que no conoces o en el cual no confías.

Assani: He escuchado que los 'Java applets' y los 'controles ActiveX' pueden ser peligrosos. Pero no tengo idea de lo que son.

Salima: Son solo ejemplos de prácticamente lo mismo: pequeños programas que tu navegador Web a veces descarga junto con la página que estás leyendo. Los diseñadores de páginas web los utilizan para crear sitios complejos, pero estos pueden también esparcir virus y software espía (spyware). No tienes porque preocuparte mucho sobre la forma como funcionan, mientras tengas el NoScript instalado y ejecutándose adecuadamente.

Cortafuegos (Firewall)

Un *cortafuegos (firewall)* [20] es el primer programa que encuentran los datos entrantes de Internet. También es el último programa que maneja la información saliente. Como un guardia de seguridad, ubicado en la puerta de un edificio que decide quién ingresa y quién puede salir, un cortafuegos (firewall) recibe, inspecciona y toma decisiones respecto a la entrada y salida de todos los datos. Naturalmente, es indispensable que te defiendas de conexiones no confiables de Internet y de redes locales, las cuales pueden proporcionar a los *piratas informáticos (hackers)* [1] y a los virus una ruta libre a tu computadora. Sin embargo, el vigilar las conexiones de salida que se originan en tu computadora no es menos importante.

Un buen *cortafuegos (firewall)* [20] te permite elegir permisos de acceso para cada programa en tu computadora. Cuando uno de estos programas intenta contactarse con el exterior, tu cortafuegos (firewall) bloqueará el intento y te enviará una advertencia, a menos que reconozca el programa y verifique que le has dado permiso para que haga ese tipo de conexión. Esto es en gran parte para prevenir que el *software malicioso (malware)* [2] existente esparza virus o invite a los *piratas informáticos (hackers)* [1] a ingresar a tu computadora. En este sentido, un cortafuegos (firewall) funciona tanto como una segunda línea de defensa o como un sistema de alerta temprana que puede ayudarte a reconocer cuando la seguridad de tu computadora esta amenazada.

Software Cortafuegos (Firewall)

Las últimas versiones del Microsoft Windows incluyen un *cortafuegos (firewall)* [20] incorporado, que se activa automáticamente. Lamentablemente, el cortafuego de Windows es limitado en muchas formas; por ejemplo no examina las conexiones de salida. Sin embargo, existe un excelente programa de *software gratuito (freeware)* [7] llamado *Comodo Firewall* [5], que realiza mejor el trabajo de mantener segura tu computadora.

Parte Práctica: Empieza con la Guía del Comodo Firewall [21]

Evitar conexiones no confiables a red

- Sólo instala programas esenciales que usas para trabajo sensible en tu computadora y asegúrate de obtenerlos de fuentes confiables, Desinstala cualquier software que no utilices.

- Desconecta tu computadora de la Internet cuando no la estés utilizando y desconéctala completamente durante la noche.
- No compartas con nadie tu contraseña de Windows.
- Si has habilitado cualquier de los 'servicios de Windows' que ya no estás utilizando, debes deshabilitarlos. Dirígete a la sección de **Lecturas Adicionales** [22] para más detalles sobre esto
- Asegúrate que todas las computadoras de la red de tu oficina tengan instaladas un *cortafuegos (firewall)* [20]
- Si todavía no tienes uno, debes considerar instalar un cortafuegos (firewall) adicional para proteger la totalidad de la red local en tu oficina. Muchas de las *pasarelas (gateways)* [23] comerciales de banda ancha incluyen un cortafuegos (firewall) fácil de utilizar, y el ejecutarlo puede mejorar de manera importante la seguridad de tu red. Si no estás seguro como empezar con esto, quizá quieras solicitar asistencia a la persona o empresa que configuró tu red.

Asani: De modo que ahora, ¿quieren que instale un antivirus, un software contra software espía (spyware) y un software cortafuegos (firewall)? ¿Puede mi computadora soportar todo eso?

Muhindo: Absolutamente. De hecho, estas tres herramientas son el mínimo indispensable si deseas mantenerte a salvo actualmente en la Internet. Éstos se han creado para trabajar juntos, de modo que el instalarlos todos no debe causarte ningún problema. Sin embargo, recuerda, no deseas ejecutar dos programas antivirus o dos cortafuegos (firewalls) al mismo tiempo.

Mantener actualizado tu software

Los programas de computadora son a menudo largos y complejos. Es inevitable que algunos de los programas que utilizas regularmente contengan errores no descubiertos, y es probable que algunos de estos errores puedan comprometer la seguridad de tu computadora. Sin embargo, los desarrolladores de software continúan encontrando estos errores, y por ello publican actualizaciones para arreglarlos. Por lo tanto es esencial que actualices frecuentemente todos los programas en tu computadora, incluyendo el sistema operativo. Si Windows no se actualiza automáticamente, puedes configurarlo haciendo clic en el menú de **Inicio**, seleccionando **Programas** y haciendo clic en **Windows Update**. Esto abrirá el Internet Explorer, y te conducirá a la página de Microsoft Update donde puedes habilitar la opción de **Actualizaciones Automáticas**. Dirígete a la sección **Lecturas Adicionales** [22] para aprender más acerca de esto.

Mantenerse actualizado con software libre y herramientas de software libre y de código abierto (FOSS)

El *software propietario* [24] a menudo requiere probar que fue comprado legalmente antes de permitirte instalar actualizaciones. Si estás utilizando, por ejemplo, una copia pirata de Microsoft Windows, esta puede no ser capaz de actualizarse automáticamente, lo que te dejaría a ti y a tu información extremadamente vulnerables. Al no tener una licencia válida, te pones a ti y a otros en riesgo. El confiar en software ilegal puede presentar también riesgos no técnicos. Las autoridades en un creciente número de países han empezado a verificar si las organizaciones poseen una licencia válida por cada software que utilizan. La policía ha confiscado computadoras y cerrado organizaciones basados en la 'piratería de software.' Esta justificación puede convertirse fácilmente en un abuso en países donde las autoridades tienen razones políticas para interferir en el trabajo de alguna organización determinada. Afortunadamente no tienes que comprar software costoso para protegerte de tácticas como ésta.

Te recomendamos enfáticamente que pruebes *software gratuito (freeware)* [7] o *Software Libre y de Código Abierto (FOSS)* [8] que sean alternativas a cualquier *software propietario* [24] que utilizas actualmente, especialmente a aquellos programas que no están licenciados. El software gratuito (freeware) y las herramientas de Software Libre y de Código Abierto (FOSS) son a menudo escritos por voluntarios y organizaciones sin fines de lucro que los publican, e incluso los actualizan gratuitamente. Las herramientas de Software Libre y Código Abierto (FOSS), en particular, son generalmente considerados más seguros que aquellos software propietarios, debido a que son desarrollados de manera transparente, pues permiten que su *código fuente* [25] sea examinado por un grupo diverso de expertos, cualquiera de los cuales puede identificar problemas y aportar soluciones.

Muchas aplicaciones de *Software Libre y de Código Abierto (FOSS)* [8] se ven y funcionan de manera casi idéntica al *software propietario* [24] que pretenden reemplazar. Al mismo tiempo, puedes utilizar estos programas junto con el software propietario, incluyendo el sistema operativo Windows, sin ningún problema. Incluso si tus colegas continúan utilizando la versión comercial de un tipo particular de programa, tú puedes intercambiar archivos y compartir información con ellos de manera fácil. En particular, deberías considerar reemplazar el Internet Explorer, Outlook o Outlook Express y Microsoft Office con *Firefox* [16], *Thunderbird* [26] y LibreOffice, respectivamente.

De hecho, podrías incluso dejar completamente de lado el sistema operativo Microsoft Windows, e intentar utilizar uno más seguro y alternativo de *Software Libre y de Código Abierto (FOSS)* [8] llamado *GNU/Linux* [6]. La mejor manera de saber si estás listo/a para hacer el cambio es simplemente intentándolo. Puedes descargar una versión *LiveCD* [27] de *Ubuntu Linux* [6], quemarla en un CD o DVD, ponerla en tu computadora y reiniciarla. Cuando haya terminado de cargar, tu computadora estará funcionando con GNU/Linux, y podrás decidir que hacer. No te preocupes, nada de esto es permanente. Cuando hayas concluido, simplemente apaga tu computadora y retira el Ubuntu LiveCD. La próxima vez que

la enciendas, estarás de vuelta en Windows, y todas tus aplicaciones, configuraciones y datos se encontrarán de la misma forma en la que los dejaste. Además de las ventajas de seguridad general del software de código abierto, Ubuntu tiene una herramienta de actualización libre y de fácil uso que evitará que tu sistema operativo y mucho de tu software queden desactualizados e inseguros.

Lecturas Adicionales

- Ver capítulo sobre Software mailicioso y Correo Comercial no Deseado [28] y el Anexo sobre Configuración de Programas de Navegación en Internet [29] en el libro Seguridad Digital y Privacidad para Defensores de los Derechos Humanos [30] [1].
- Manténte actualizado con las noticias sobre virus del sitio Virus Bulletin [31] [2].
- Aprende como decidir qué 'Servicios Windows' no necesitas [32] [3] y cómo deshabilitarlos [33] [4].
- Otras guías de Tactical Technology Collective (TTC [34]) [5] NGO-in-a-Box [35], te pueden ayudar a cambiar y comenzar a usar herramientas gratuitas (freeware) y Software Libre y de Código Abierto (FOSS) para todo tipo de programas que necesites
- Descarga gratuitamente CDs de arranque para rescate [36] con el fin de escanear tu computadora y eliminar los virus sin ejecutar Windows en tu computadora.
- Si crees que tu computadora está infectada con un virus u otro tipo de software malicioso lea [37]

Referencias

[1] www.frontlinedefenders.org/manual/en/esecman [38]
[2] www.virusbtn.com [39]
[3] https://security.berkeley.edu/MinStds/Determining-Un-Services-Windows.html [32]
[4] www.marksanborn.net/howto/turn-off-unnecessary-windows-services [33]
[5] www.tacticaltech.org [40]

2. Proteger tu información de amenazas físicas

No importa cuanto esfuerzo hayas puesto en construir una barrera digital alrededor de tu computadora, todavía puedes despertar una mañana y hallar que esta, o una copia de la información en ella, se ha perdido, ha sido robada, o dañada por cualquier serie de accidentes desafortunados o actos maliciosos. Cualquier cosa desde una sobretensión transitoria a una ventana abierta o una taza de café derramada puede conducirte a una situación en la cual todos tus datos se pierdan y no seas capaz de utilizar tu computadora. Una cuidadosa evaluación del riesgo, un consistente esfuerzo para mantener una computadora sin problemas y una *política de seguridad* [41] pueden evitar este tipo de desastre.

Contexto

Shingai y Rudo son una vieja pareja casada con muchos años de experiencia, que ayudan a la población infectada con el VIH en Zimbabwe a mantener su acceso a medicación apropiada. Ellos están postulando para un subsidio para comprar nuevas computadoras y equipo de red para su oficina. Dado que viven en una región que es muy turbulenta, tanto en términos políticos como de infraestructura, ellos y sus potenciales financistas quieren garantizar que su nuevo hardware estará seguro, no sólo de los piratas informáticos (hackers) y los virus, sino también de la confiscación, tormentas eléctricas, picos eléctricos y otros desastres similares. Ellos le consultaron a Otto, un técnico en computadoras local, que les ayude a concebir un plan para reforzar la seguridad física de las computadoras y de los equipos de red que planean adquirir si su solicitud de subvención tiene respuesta.

¿Qué puedes aprender de este capítulo?

- Unos cuantos ejemplos de las muchas *amenazas físicas* [42] a tu computadora y a la información que se halla almacenada en ella.
- Cómo asegurar tu computadora de la mejor forma contra estas amenazas
- Cómo crear un entorno operativo sin problemas para las computadoras y los equipos de red
- Que debes considerar cuando creas un plan de seguridad para las computadoras en tu oficina.

Evaluar tus riesgos

Muchas organizaciones subestiman la importancia de mantener seguras sus oficinas y su equipamiento físico. Como resultado de ello, a menudo carecen de una clara política que describa que medidas deben tomarse para proteger las computadoras y los dispositivos de almacenamiento de respaldos de robos, condiciones climáticas extremas, accidentes, y otras *amenazas físicas* [42]. La importancia de dichas políticas puede parecer obvia, pero el formularlas adecuadamente puede ser más complicado de lo que parece. Muchas organizaciones, por ejemplo, tienen buenas cerraduras en las puertas de sus oficinas — y muchas incluso tienen sus ventanas aseguradas — pero si no prestan atención al número de llaves que han sido creadas, y quienes las tienen, su información sensible se mantendrá vulnerable.

Shingai: Deseamos colocar un breve resumen de nuestra política de seguridad en esta solicitud de subvención, pero también necesitamos asegurarnos que la política es adecuada en si. ¿Qué debemos incluir en ella?

Otto: Me temo que no puedo recomendarle una solución general al reto de la seguridad física. Los detalles de una buena política casi siempre dependen de las circunstancias individuales de la organización en particular. Sin embargo, aquí le brindo algunas consejos generales: cuando intente elaborar un plan, debes observar tu ambiente de trabajo de manera cuidadosa y pensar creativamente sobre donde podrían estar tus puntos débiles y que puedes hacer para fortalecerlos.

Cuando estés evaluando los riesgos y las vulnerabilidades que tú y tu organización afrontan, debes evaluar varios niveles diferentes en los que tus datos pueden estar amenazados.

- Considera los canales de comunicación que usas y cómo lo haces. Ejemplos de ello pueden incluir cartas físicas, faxes, teléfonos fijos, teléfonos móviles, correos electrónicos y mensajes a través de *Skype* [43].
- Considera cómo almacenas información importante. Los discos duros de las computadoras, los correos electrónicos y los servidores web, las memorias extraíbles USB, los discos duros externos con conexión USB, los CDs y DVDs, los teléfonos móviles, el papel impreso y las notas manuscritas son todas posibilidades.
- Considera donde están ubicados físicamente estos artículos. Pueden estar en la oficina, en la casa, en un bote de basura afuera o, en forma creciente, 'en algún lugar de la Internet.' En este último caso, podría ser todo un reto determinar la ubicación física actual de una pieza particular de información.

Ten en cuenta que la misma pieza de información podría ser vulnerable en distintos niveles. De la misma manera como tú podrías confiar en un software antivirus para proteger los contenidos de una memoria extraíble USB de *software malicioso (malware)* [2], así también debes confiar en un plan de seguridad física detallado para proteger la misma información del robo, perdida o destrucción. Aunque algunas prácticas de seguridad, tales como tener una buena política de mantener respaldos fuera del lugar de trabajo, son útiles contra amenazas digitales y físicas, otras son claramente más específicas.

Cuando decides llevar tu memoria extraíble USB en el bolsillo o sellada en una bolsa plástica al fondo de tu maleta, estás tomando una decisión de seguridad física, aun cuando la información que tratas de proteger sea digital. Como es normal, la política correcta depende en gran parte de la situación. ¿Estás caminando a través de un pueblo o a través de una frontera? ¿Alguien estará cargando tu bolso o mochila? ¿Está lloviendo? Estas son algunas preguntas que debes tener en cuenta cuando tomes una decisión como esta.

Proteger tu información de intrusos físicos

Los individuos maliciosos que buscan tener acceso a tu información sensible representan una clase importante de *amenaza física* [42]. Sería un error asumir que ésta es la única amenaza física a la seguridad de tu información, pero sería aún peor el ignorarla. Existen varios pasos que puedes tomar para ayudar a reducir el riesgo de intrusión física. Las categorías y sugerencias que se presentan a continuación, muchas de las cuales pueden funcionar tanto para tu domicilio como para tu oficina, representan una base sobre la cual puedes desarrollar otras de acuerdo a tu particular situación de seguridad física.

Alrededor de la Oficina

- Conoce a tus vecinos. Dependiendo del clima de seguridad en tu país y en tu vecindario, una de dos cosas puede ser posibles. Ya sea que, puedas volverlos aliados que te ayudarán a cuidar tu oficina, o personas a las que debes añadir a tu lista de amenazas potenciales y de las cuales debes ocuparte en tu plan de seguridad.
- Revisa como proteges todas tus puertas, ventanas y otros puntos de entrada que conduzcan a tu oficina.
- Considera instalar una cámara de vigilancia o una alarma con sensor de movimiento.
- Trata de crear un área de recepción, donde los visitantes puedan ser atendidos antes de que ingresen a la oficina, y una sala de reuniones que esté separada de los espacios de trabajo.

En la Oficina

- Protege los cables de red haciéndolos pasar por dentro de la oficina.
- Mantén bajo llave los dispositivos de red como *servidores* [44], *enrutadores (routers)* [23], *interruptores* [23], *concentradores (hubs)* [23], y módems en habitaciones o gabinetes seguros. Un intruso con acceso físico a dicho equipo puede instalar software malicioso (malware) [2] capaz de robar datos en tránsito o atacar otras computadoras en la red incluso después de que se haya ido. En algunas circunstancias es preferible esconder los servidores, computadoras y otro equipo en áticos, en cielorasos falsos, o incluso con un vecino, y utilizarlos a través de una conexión inalámbrica.
- Si tienes una red inalámbrica, es esencial que asegures tu *punto de acceso* [23] de modo que los intrusos no puedan unirse a tu red o vigilar tu tráfico. Si estas utilizando una red inalámbrica insegura, cualquiera con una computadora portátil en tu vecindario se convierte en un intruso potencial. Es una definición inusual de riesgo 'físico,' pero ayuda el considerar que un individuo malicioso que pueda vigilar tu red inalámbrica tiene el mismo acceso que uno que pueda ingresar furtivamente en tu oficina y conectar un cable ethernet. Los pasos necesarios para asegurar una red inalámbrica variaran, dependiendo de tu punto de acceso, tu hardware y software, pero son raramente difíciles de seguir.

En tu área de trabajo

- Debes ubicar con cuidado la pantalla de tu computadora, tanto en tu escritorio como cuando estas fuera de la oficina, con el fin de evitar que otros lean los que se muestra en ella. En la oficina, esto significa considerar la ubicación de las ventanas, puertas abiertas y el área de espera de los invitados, si es que cuentas con una.
- La mayoría de las torres de las computadoras de escritorio tiene una ranura donde puedes colocar un candado que impedirá a alguien sin una llave tener acceso a su interior. Si tienes torres como esta en la oficina, debes colocarles candados de modo que los intrusos no puedan alterar el hardware interno. Esta característica debe ser considerada al momento de comprar nuevas computadoras.
- Utiliza un cable de seguridad de cierre, cuando sea posible, para evitar que intrusos puedan robar las computadoras. Esto es especialmente importante para computadoras portátiles y pequeñas computadoras de escritorio que pueden ser escondidas en una bolsa o bajo un abrigo.

Software y configuraciones relacionadas a la seguridad física

- Asegúrate que cuando reinicies tu computadora, ésta te solicite una contraseña antes de permitirte ejecutar un software y acceder a archivos. Si no lo hace, puedes habilitar esta opción en Windows haciendo clic en el Menú de Inicio, Configuración, seleccionar el Panel de Control, y doble clic en Cuentas de Usuario. En la pantalla de Cuentas de Usuario, selecciona tu cuenta y haz clic en Crear una Contraseña. Elige una contraseña segura como se aborda en el capítulo **3. Crear y mantener contraseñas seguras** [45], ingresa tu contraseña, confírmala, haz clic en Crear Contraseña y haz clic en Si, Hacerla Privada (Make Private).
- Existen pocas opciones en el *BIOS* [46] de tu computadora que son pertinentes para la seguridad física. Primero, debes configurar tu computadora de modo que no *arranque* [47] desde un dispositivo USB, CD-ROM o DVD. Segundo, debes fijar una contraseña en el mismo BIOS, de modo que un intruso no pueda simplemente deshacer la configuración previa. Nuevamente, asegúrate de elegir una contraseña segura.
- Si confías en una base de datos de contraseñas seguras, como se aborda en el **capítulo 3** [45], para almacenar tus contraseñas de Windows o del BIOS para una computadora en particular, asegúrate de no guardar una única copia de la base de datos en dicha computadora.
- Adquiere el hábito de cerrar tu cuenta cada vez que te alejes de tu computadora. En Windows, puedes hacer esto rápidamente manteniendo presionada la tecla con el logo de Windows y presionando la tecla L. Ello solo funcionará si has creado una contraseña para tu cuenta, como se describió anteriormente.
- *Cifra* [48] la información sensible en tus computadoras y dispositivos de almacenamiento en tu oficina. Dirígete al capítulo **4. Proteger los archivos sensibles en tu computadora** [49] para obtener detalles e indicaciones adicionales en las Guías Prácticas pertinentes.

Rudo: Estoy un poco nervioso en cuanto a equivocarme en el BIOS. ¿Podría arruinar mi computadora si cometo algún error?

Otto: Si puedes, al menos por un instante. De hecho, las opciones que desearías cambiar son muy simples, pero la pantalla del BIOS puede ser un poco intimidante, y es posible dejar tu computadora temporalmente incapaz de arrancar si cometes algún error. En general, si no te sientes cómodo trabajando en el BIOS, debes pedir a alguien con mayor experiencia con computadoras que te ayude.

Dispositivos Portátiles

- Mantén tu computadora portátil, tu teléfono móvil y otros dispositivos portátiles que contengan información sensible

todo el tiempo contigo, especialmente si estas viajando o te estas alojando en un hotel. El viajar con un *cable de seguridad* [50] para computadora portátil es una buena idea, aunque a veces es difícil encontrar un objeto apropiado al cual puedas fijarlo. Recuerda que las horas de toma de alimentos son a menudo aprovechadas por los ladrones, muchos de los cuales han aprendido a revisar habitaciones de hotel en busca de computadoras portátiles durante las horas del día cuando estas están probablemente sin vigilancia.
- Si tienes una computadora portátil, una tablet o dispositivo móvil, trata de evitar ponerlos a vista de todos. No hay necesidad de mostrar a los ladrones que estas llevando valioso hardware o de mostrarles a los individuos que pudieran desear acceder a tus datos que tu mochila contiene un disco duro lleno de información. Evita usar tus dispositivos portátiles en áreas públicas, y considera llevar tu computadora portátil en algo que no se vea como una bolsa para computadoras portátiles.

Mantener un ambiente sano para el hardware de tu computadora

Como muchos dispositivos electrónicos, las computadoras son muy sensibles. No se adaptan bien a suministros eléctricos inestables, temperaturas extremas, polvo, alto grado de humedad o esfuerzo mecánico. Existen muchas cosas que puedes hacer para proteger a tu computadora y equipo de red de dichas amenazas:

- Los problemas eléctricos tales como sobrecargas de energía, apagones y bajas de tensión pueden causar daño físico a una computadora. Las irregularidades como éstas pueden 'arruinar' tu disco duro, dañar la información que contiene, o dañar físicamente los componentes eléctricos en tu computadora.
    - Si puedes costearlas, debes instalar dispositivos de *Corriente Eléctrica Ininterrumpida* [51] (UPS por sus siglas en inglés) a las computadoras más importantes de tu oficina. Un UPS estabiliza el suministro eléctrico y provee energía temporal en caso de apagón.
    - Incluso donde las *UPSs* [51] se consideran inapropiadas o muy costosas, puedes proporcionar filtros de energía o protectores contra sobretensiones, cualquiera de los cuales ayudará a proteger tus equipos de sobrecargas de energía.
    - Prueba tu red eléctrica antes de conectar equipos importantes a ella. Trata de usar enchufes que tengan tres ranuras, una de ellas 'a tierra.' Y, si es posible, tómate un día o dos para ver cómo se comporta el sistema eléctrico en una nueva oficina cuando está dando energía a dispositivos baratos, tales como lámparas y ventiladores, antes de poner tus computadoras en riesgo.
- Para protegerse contra los accidentes en general, evita colocar hardware importante en pasillos, áreas de recepción, u otras ubicaciones de fácil acceso. Los *UPSs* [51], filtros de energía, protectores contra sobretensiones, regletas y cables de extensión — particularmente aquellos conectados a los servidores y al equipo en red — deben estar ubicados donde no puedan ser apagados por un traspié accidental.
- Si tienes acceso a cables de computadora, regletas y extensiones de alta calidad, debes comprar suficientes para servir a toda la oficina y contar con algunos extras. Las regletas que se desprenden de los enchufes de las paredes y producen chispas constantemente son más que molestos. Estos pueden ser muy perjudiciales para la seguridad física de cualquier computadora que esté conectada a este. Ello puede conducir a que usuarios frustrados aseguren sus cables sueltos a las regletas utilizando cinta adhesiva, lo cual crea un obvio peligro de incendio.
- Si mantienes alguna de tus computadoras dentro de un gabinete, asegúrate que tengan ventilación adecuada, porque sino se pueden sobrecalentar.
- El equipo de computación no debe ser ubicado cerca de radiadores, rejillas de la calefacción, aire acondicionado u otros mecanismos con conductos

Shingai: En realidad, ya resolvimos algunos de esos problemas a inicios de este año. Pasamos meses intentando encontrar cables que no cayeran fuera de la parte posterior de nuestras computadoras.

Otto: ¿Y, regletas que no parecieran que estuvieran a punto de incendiar la alfombra?

Shingai: Eso también. Al final, Rudo tuvo que traer algunos de regreso de su viaje a Johannesburgo. Fíjate, la electricidad en sí es todavía muy inestable, pero al menos el equipo es fácil de manipular.

Crear tu política de seguridad física

Una vez que hayas evaluado las amenazas y las vulnerabilidades que tú y tu organización afrontan, debes considerar los pasos que deben tomar para mejorar su seguridad física. Debes crear una *política de seguridad* [41] detallada poniendo por escrito estos pasos. El documento resultante servirá como una guía general para ti, tus colegas y cualquier persona nueva en tu organización. Este documento también debe proporcionar una lista de verificación de acciones a ser tomadas ante la ocurrencia de varias emergencias de seguridad física. Todos los involucrados deben tomarse el tiempo necesario para leerlo, implementarlo y cumplir con estas normas de seguridad. Ellos también deben ser alentados a realizar preguntas y proponer sugerencias de cómo mejorar el documento.

Tu *política de seguridad* [41] física puede contener varias secciones, dependiendo de las circunstancias:

- Una política de ingreso a la oficina que se ocupe de los sistemas de alarma, cuantas llaves existen y quienes las tienen, cuando se admiten invitados en la oficina, quienes tienen el contrato de limpieza y otros asuntos pertinentes
- Una política sobre que partes de la oficina deben estar restringidas a visitantes autorizados.
- Un inventario de tu equipo, incluyendo los números de serie y las descripciones físicas.
- Un plan para la disposición segura de papeles que contengan información sensible
- Procedimientos de emergencia relacionados a:
    - Quién debe ser notificado en caso que información sensible sea revelada o extraviada
    - A quién contactar en caso de incendio, inundación, u otro desastre natural.
    - Cómo ejecutar ciertas reparaciones clave de emergencia.
    - Cómo contactar a las compañías u organizaciones que proporcionan servicios tales como energía eléctrica, agua y acceso a Internet.
    - Cómo recuperar información de tu sistema de respaldo externo. Puedes hallar consejos más detallados sobre copias de respaldo en el capítulo **5. Recuperar información perdida** [52].

Tu *política de seguridad* [41] debe ser revisada y modificada periódicamente para reflejar cualquier cambio en la política que se haya realizado desde la última revisión. Y por supuesto, no olvides respaldar tu documento de política de seguridad junto con el resto de tus datos importantes. Dirígete a la sección de **Lecturas Adicionales** [53] para mayor información sobre la creación de una política de seguridad.

Lecturas Adicionales

- Para información adicional sobre evaluación de riesgos, dirígete a las secciones de Conciencia de Seguridad [54], y Círculo de Seguridad y Evaluación de Amenazas [55] del libro Seguridad Digital y Privacidad para Defensores de los Derechos Humanos [38] [1].
- Para una explicación más detallada sobre cómo fijar una contraseña para el BIOS, dirígete al capítulo de Seguridad de Windows [56] en el libro Seguridad Digital y Privacidad para Defensores de los Derechos Humanos [38] [1].
- Para hallar guías sobre creación de políticas de seguridad, dirígete a Caso de Estudio 1 [57] en el libro Seguridad Digital y Privacidad para Defensores de los Derechos Humanos [38] [1].
- También revisa el Manual de Protección [58] y el Libro de Protección [59] para Defensores de los Derechos Humanos [2].

Referencias

[1] www.frontlinedefenders.org/manual/en/esecman [38]
[2] www.frontlinedefenders.org/manuals [60]

3. Crear y mantener contraseñas seguras

Muchos de los servicios seguros que nos permiten sentirnos cómodos utilizando la tecnología digital para conducir negocios importantes, desde ingresar a nuestras computadoras y enviar correos electrónicos hasta *cifrar* [48] y esconder datos sensibles, requieren que recordemos una contraseña. Estas palabras secretas, frases o secuencias en auténtico galimatías a menudo proporcionan la primera, y a veces la única, barrera entre tu información y cualquiera que pudiera leerla, copiarla, modificarla o destruirla sin permiso. Existen muchas maneras por las cuales alguien puede descubrir tus contraseñas, pero puedes defenderte de la mayoría de ellos aplicando unas cuantas tácticas y por medio de una herramienta de *base de datos de contraseñas seguras* [61], tales como el *KeePass* [62].

Contexto

Mansour y Magda son dos hermanos, en un país de habla árabe, quiénes mantienen una bitácora (blog) en la cual anónimamente hacen difusión sobre abusos de los derechos humanos y hacen campañas para un cambio político. Magda recientemente trató de conectarse a su cuenta de correo con interfase web y se encontró con que su contraseña había sido modificada. Después de reestablecer la contraseña, ella fue capaz de conectarse, pero cuando abrió su buzón encontró que muchos mensajes nuevos fueron marcados como leídos. Ella sospecha que alguien afiliado a una organización de adversarios políticos pudiera haber descubierto o adivinado su contraseña, la cual utiliza para prácticamente todas sus cuentas web. Ella se reúne con Mansour, que tiene menor experiencia con computadoras, para explicarle la situación y expresarle su preocupación.

¿Qué puedes aprender de este capítulo?

- Los elementos de una contraseña segura
- Unos cuantos trucos para recordar contraseñas largas y complicadas
- Cómo utilizar la *base de datos de contraseñas seguras* [61] del *KeePass* [62] para almacenar contraseñas en vez de recordarlas

Seleccionar y mantener contraseñas seguras

En general, cuando deseas proteger algo, lo cierras con una llave. Las cerraduras de las casas, automóviles y bicicletas tienen llaves físicas; los archivos protegidos tienen llaves de *cifrado* [48]; las tarjetas bancarias tiene números PIN; y las cuentas de correo electrónico tienen contraseñas. Todas estas llaves, en forma literal y metafórica, tienen una cosa en común: abren sus respectivas cerraduras con la misma eficacia en manos de otra persona. Puedes instalar cortafuegos avanzados, cuentas de correo electrónico seguras, y discos cifrados, pero si tu contraseña es muy débil, o si permites que caiga en las manos equivocadas, ello no te hará mucho bien.

Elementos de una contraseña sólida

Una contraseña debe ser difícil de adivinar para un programa de computadora.

- **Debe ser larga**: Cuanto más larga es la contraseña es menos probable que sea adivinada por un programa de computadora en un tiempo razonable. Debes tratar de crear contraseñas que incluyan diez o más caracteres. Algunas personas utilizan contraseñas que contienen más de una palabra, con o sin espacios, las cuales son a menudo llamadas frases contraseña. Esta es una buena idea, en la medida que el programa o servicio que utilices te permita elegir contraseñas lo suficientemente largas.
- **Debe ser compleja**: Además de ser extensa, la complejidad de una contraseña también ayuda a evitar que el software automático de 'descifrado de contraseñas' adivine la correcta combinación de caracteres. Donde sea posible, siempre debes incluir en tu contraseña letras en mayúsculas, en minúsculas, números, y símbolos tales como signos de puntuación.

Una contraseña debe ser difícil de descifrar para otros.

- **Debe ser práctica:** Si has escrito tu contraseña debido a que no puedes recordarla, podrías terminar afrontando una completamente nueva categoría de amenazas que te podría dejar vulnerable ante cualquiera con una clara vista de tu escritorio o acceso temporal a tu domicilio, tu billetera, o incluso el bote de basura fuera de tu oficina. Si eres incapaz de pensar en una contraseña que sea larga y compleja pero a la vez factible de ser recordada, la sección **Recordar y registrar contraseñas seguras** [63], que viene a continuación, podría ser de ayuda. Sino, debes todavía escoger algo seguro, pero necesitas registrarla utilizando una *base de datos de contraseñas seguras* [61] tal como *KeePass* [62]. Otros tipos de archivos protegidos por contraseña, incluyendo documentos de Microsoft Word, no debe ser confiados para este propósito, debido a que muchos de ellos pueden ser descifrados en segundos utilizando herramientas que son de libre acceso en Internet.
- **No debe ser personal:** Tu contraseña no debe estar relacionada a ti de manera personal. No elijas una palabra o frase que se origina de información como tu nombre, número de seguridad social, número de teléfono, nombre de tu hijo(a), nombre de tu mascota, fecha de nacimiento, o cualquier otra cosa que una persona podría descubrir haciendo una pequeña investigación sobre ti.
- **Debe mantenerse secreta:** No compartas tu contraseña con nadie a menos que sea absolutamente necesario. Y, si debes compartir una contraseña con un amigo, miembro de la familia o colega, debes cambiarla a una contraseña temporal primero, compartir esta, luego cambiarla nuevamente cuando la persona haya terminado de utilizarla. A menudo, existen alternativas para compartir una contraseña, tal como crear una cuenta separada para cada miembro que necesite acceso. El mantener tu contraseña secreta también implica poner atención a quién podría estar fisgoneándote cuando la ingresas o buscas en una *base de datos de contraseñas seguras* [61].

Una contraseña debe ser escogida de modo que se minimice el daño si alguien la descubre.

- **Hazla única:** Evita usar la misma contraseña para más de una cuenta. De otro modo, cualquiera que descubra dicha contraseña tendrá acceso a incluso mayor información sensible. Esto es particularmente cierto debido a que ciertos servicios hacen relativamente simple descifrar tu contraseña. Si utilizas, por ejemplo, la misma contraseña para tu cuenta de usuario de Windows y para tu cuenta de Gmail, alguien con acceso físico a tu computadora puede descifrar la primera y utilizarla para acceder a la segunda. Por razones similares, es una mala idea el rotar contraseñas intercambiándolas entre diferentes cuentas.
- **Mantenla siempre nueva:** Cambia tu contraseña de manera regular, de manera preferente una vez cada tres meses. Algunas personas son muy apegadas a una contraseña en particular y nunca la cambian. Esta es una mala idea. Cuanto más tiempo mantienes una contraseña, existe mayor oportunidad de que otros la descubran. Además, si alguien es capaz de utilizar tu contraseña (robada) para acceder a tu información y servicios sin que lo sepas, está continuará haciéndolo hasta que la cambias.

Mansour: ¿Qué ocurre en el caso que confíe en una persona? Está bien si te confío mi contraseña, ¿cierto?

Magda: Bueno, en primer lugar, solo porque confíes en alguien para darle tu contraseña no significa que confíes en esa persona para cuidar de ella, ¿cierto? Aunque yo no haría nada malo con tu contraseña, podría escribirla y perderla o cualquier otra cosa. Después de todo, ¡esa podría ser la forma como me metí en este problema! Además, no todo es cuestión de confianza. Si tú eres la única persona que conoce la contraseña, entonces no tienes que perder el tiempo preocupándote de a quién culpar si alguien entró sin autorización a tu cuenta. En este momento, por ejemplo, en vez de estar interrogándolos, estoy casi seguro que alguien en realidad adivinó o 'descifró' mi contraseña.

Recordar y registrar contraseñas seguras

Examinando la lista de sugerencias dada anteriormente, te preguntarás cómo puede alguien sin memoria fotográfica estar al tanto de contraseñas que son largas, complejas y sin sentido, si es que no las escribe. La importancia de utilizar diferentes contraseñas para cada cuenta lo hace aún más difícil. Sin embargo, existen algunos trucos que pueden ayudarte a crear contraseñas que son fáciles de recordar pero extremadamente difíciles de adivinar, incluso para una persona inteligente utilizando un programa avanzado de 'descifrado de contraseñas'. También tienes la opción de registrar tus contraseñas utilizando una de las *bases de datos de contraseñas seguras* [61], tal como el *KeePass* [62], que fue específicamente creado para este propósito.

Recordar contraseñas seguras

Es importante utilizar diferentes tipos de caracteres cuando escojas una contraseña. Esto se puede realizar de distintas maneras:

- Utilizando mayúsculas y minúsculas, tal como: 'Mi nomBRE NO es SR. MarSter?'
- Intercalando números y letras, tal como: 'a11 w0Rk 4nD N0 p14Y'
- Incorporando ciertos símbolos, tal como: 'c@t(heR1nthery3'
- Utilizando diferentes idiomas, tal como: 'Let Them Eat 1e gateaU du ch()colaT'

Cualquiera de estos métodos puede ayudarte a incrementar la complejidad de una contraseña. Obviamente, esto no hará fácil de recordar una contraseña normal, pero te permitirá elegir una contraseña más segura sin tener que entregarte completamente a la idea de memorizarla por completo. Algunas de las sustituciones más comunes (tales como utilizar cero en vez de una 'o' o el símbolo '@' en lugar de 'a') fueron hace mucho incorporados en las herramientas de descifrado de contraseñas, pero aún así son todavía una buena idea. Estas incrementan la cantidad de tiempo que dichas herramientas requerirían para descubrir la contraseña y, en las situaciones más comunes en las que herramientas de esta clase no pueden ser utilizadas, estás evitan las afortunadas adivinanzas.

Las contraseñas pueden también aprovechar las ventajas de *códigos nemotécnicos* [64] más tradicionales, tales como el uso de acrónimos. Esto permite que largas frases se conviertan en palabras complejas y prácticamente aleatorias:

- '¿Ser o no ser? Esa es la pregunta' se convierte en 'So-S?ElaP'
- 'Sostenemos como evidentes por sí mismas dichas verdades: que todos los hombres son creados iguales' se convierte en 'Scepsmdv:q'thsc=s'
- '¿Estás feliz hoy?' se convierte en 'tas:-)h0y?'

Estos son sólo unos cuantos ejemplos para ayudarte a desarrollar tu propio método de cifrar palabras y frases para hacerlas simultáneamente complejas y memorables.

Registrar contraseñas de forma segura

Mientras que un poco de creatividad te permitirá recordar todas tus contraseñas, la necesidad de cambiarlas periódicamente significa que muy pronto se te puede acabar la creatividad. Como alternativa, puedes generar contraseñas aleatorias y seguras para la mayoría de tus cuentas y simplemente dedicarte a recordarlas todas. En lugar de ello, puedes registrarlas en una *base de datos de contraseñas seguras* [65] portátil y cifrada tal como el *KeePass* [62].

Parte Práctica: Empieza con la Guía del KeePass [66]

Por supuesto, si utilizas este método, se hace especialmente importante que creas y recuerdes una contraseña muy segura para el *KeePass* [62], o cualquiera que sea la herramienta que elijas. Cuando sea que necesites ingresar una contraseña para una cuenta específica, puedes encontrarla utilizando sólo tu contraseña maestra, la cual hace más fácil seguir todas las sugerencias que se hicieron anteriormente. El KeePass es también portátil, lo que significa que también puedes colocar tu base de datos en una memoria extraíble USB en caso necesites buscar contraseñas cuando estás

alejado de tu computadora principal.

Aunque es probablemente la mejor opción para cualquiera que tenga que mantener un gran número de cuentas, existen algunos inconvenientes para este método. Primero, si pierdes o accidentalmente borras tu única copia de tu base de datos de contraseñas, no tendrás más acceso a ninguna de tus cuentas de las cuales esta tenía la contraseña. Esto hace extremadamente importante que hagas una copia de seguridad o respaldo de tu base de datos del *KeePass* [62]. Revisa el capítulo **5. Recuperar información perdida** [52] para mayor información sobre estrategias para la copia de seguridad o respaldo. Felizmente, el hecho que tu base de datos esté cifrada significa que no tienes que entrar en pánico si pierdes tu memoria extraíble USB o una unidad de respaldo que contenga una copia de este.

El segundo gran inconveniente podría ser más importante. Si olvidas tu contraseña maestra del *KeePass* [62], no existe un modo de recuperarla o recuperar los contenidos de tu base de datos. Por tanto, ¡asegúrate de escoger una contraseña maestra que sea tanto segura como memorable!

Mansour: Espera un minuto. Si el KeePass utiliza una sola contraseña maestra para proteger todas tus demás contraseñas, ¿cómo es más seguro que simplemente utilizar la misma contraseña para todas tus cuentas? Es decir, si una mala persona toma conocimiento de mi contraseña maestra, entonces tendrá acceso a todo, ¿cierto?

Magda: Es un buen razonamiento, y tienes razón al decir que proteger tu contraseña maestra es en verdad importante, pero existen un par de diferencias claves. En primer lugar, esta 'mala persona' no solo necesitaría tu contraseña, él también necesitaría tu archivo de base de datos del KeePass. Si tú simplemente compartes la misma contraseña con todas tus cuentas, el simplemente necesitaría sólo tu contraseña. Más importante aún, sabemos que el KeePass es extremadamente seguro ¿verdad?. Entonces otros programas y sitos web pueden ir en cualquier dirección. Algunos de ellos son mucho menos seguros que otros, y no quieres que alguien entre a un sitio débil, y luego llevar lo que aprendió para acceder a una cuenta más segura. Y hay otro tema, KeePass hace que sea fácil cambiar tu contraseña maestra si lo crees necesario. ¡Sería tan afortunado! Me pasé todo el día actualizando mis contraseñas.

Lecturas Adicionales

- Dirígete al capítulo de Protección de Contraseñas [67] y al Apéndice de ¿Cuán larga debe ser mi contraseña? [68] en el libro Seguridad Digital y Privacidad para Defensores de los Derechos Humanos [30] [1].
- Wikipedia tiene interesantes artículos sobre Contraseñas [69] [2] , Guías para fortalecer contraseñas [70] [3], y descifrado de contraseñas [71] [4].

Referencias

[1] www.frontlinedefenders.org/manual/en/esecman [38]
[2] www.en.wikipedia.org/wiki/Password [72]
[3] www.en.wikipedia.org/wiki/Password_strength [73]
[4] www.en.wikipedia.org/wiki/Password_cracking [74]

4. Proteger los archivos sensibles en tu computadora

El acceso no autorizado a la información en tu computadora o dispositivo de almacenamiento portátil puede llevarse a cabo de manera remota, si el 'intruso' es capaz de leer o modificar tus datos a través de la Internet, o físicamente, si logra conectarse con tu hardware. Puedes protegerte de cualquiera de estos tipos de amenaza mejorando la seguridad física y de la red de tu datos, como se trató en el capítulo **1. Proteger tu computadora de software malicioso (malware) y de piratas informáticos (hackers)** [75] y en el capítulo **2. Proteger tu información de amenazas físicas** [76].

Sin embargo, es siempre mejor tener varios niveles de defensa, razón por la cual debes proteger también los archivos mismos. De esta manera, es probable que tu información sensible se mantenga a salvo incluso si tus otras iniciativas en seguridad resultan ser inadecuadas.

Existen dos enfoques generales frente al reto de dar seguridad a tus datos en esta forma. Puedes *cifrar* *[48]* tus archivos, haciéndolos ilegibles a cualquiera que no sea tú, o puedes esconderlos confiando en que un intruso será incapaz de encontrar tu información sensible. Existen herramientas que te ayudan con cualquiera de los enfoques, incluyendo una aplicación que es un *Software Libre y de Código Abierto (FOSS)* [8] llamado *TrueCrypt* [77], que puede tanto cifrar como esconder tus archivos.

Contexto

Claudia y Pablo trabajan con una ONG de derechos humanos en un país de Sudamérica. Ellos han pasado muchos meses recolectando testimonios de testigos de violaciones de los derechos humanos que fueron cometidos por el ejército en su región. Si los detalles de quién proporcionó estos testimonios se hacen conocidos se pondría en peligro tanto a la valerosa gente que testificó, como a los miembros de la organización en dicha región.

Esta información está actualmente almacenada en una hoja de cálculo en la computadora de la ONG que funciona con Windows XP, la cual está conectada a Internet.Siendo concientes de la seguridad, Claudia se ha asegurado de almacenar en un CD una copia de respaldo de los datos, este se mantiene fuera de la oficina.

¿Qué puedes aprender de este capítulo?

- Cómo *cifrar* [48] información en tu computadora
- Cuales son los riesgos que podrías afrontar manteniendo tus datos cifrados
- Cómo proteger datos en memorias extraíbles USB, en caso estas se pierdan o sean robadas
- Que pasos debes dar para esconder información de intrusos físicos y remotos

Cifrar tu información

Pablo: ¡Pero mi computadora ya está protegida por la contraseña de acceso de Windows! ¿No es eso lo suficientemente bueno?

Claudia: En realidad, las contraseñas de acceso de Windows son normalmente muy fáciles de descifrar. Además, cualquiera que ponga sus manos en tu computadora por el tiempo suficiente para reiniciar tu computadora con un LiveCD en la unidad lectora puede copiar tus datos sin siquiera tener que preocuparse sobre la contraseña. Si esta persona logra llevarse la computadora por un momento te encontrarás en peores problemas. Por ello no es sólo la contraseña de Windows de lo que necesitas preocuparte. Tampoco debes confiar en las contraseñas de Microsoft Word o de Adobe Acrobat.

El *cifrar* [48] tu información se parece un poco a mantenerla encerrada en una caja fuerte. Sólo aquellos que tengan la llave o conozcan la combinación de la cerradura pueden acceder a ella. La analogía es particularmente apropiada para el *TrueCrypt* [77] y herramientas similares, las cuales crean contenedores seguros llamados 'volúmenes cifrados' en vez de simplemente proteger un archivo a la vez. Puedes poner un gran número de archivos dentro de un volumen cifrado, pero estas herramientas no protegerán los archivos que estén almacenados en otro lugar en tu computadora o en tu memoria extraíble USB.

Parte Práctica: Empieza con la Guía del TrueCrypt [78]

Mientras que otro software puede proporcionarte un *cifrado* [48] que sea igualmente fuerte, *TrueCrypt* [77] contiene varias características importante que te permitirá diseñar tu estrategia de seguridad informática. Te da la posibilidad de encriptar permanentemente todo el disco de tu computadora incluyendo todos tus archivos, todos tus archivos temporales creados durante tu trabajo, todos los programas que hayas instalado y todos los archivos del sistema operativo Windows. Truecrypt proporciona respaldo para llevar volúmenes cifrados en dispositivos portátiles de almacenamiento. Y provee la opción de 'denegación' descrita en la sección **Ocultar tu información sensible** [79]. Adicionalmente TrueCrypt es un programa de gratuito y de código abierto.

Pablo: Está bien, ahora si que me tienes preocupado. ¿Qué sucede con los otros usuarios de la misma computadora? ¿Esto significa que pueden leer documentos en la carpeta de 'Mis Documentos'?

Claudia: ¡Me gusta la manera en la que piensas! Si tu contraseña de Windows no te protege de los intrusos ¿cómo te podría proteger de otras personas con cuentas en la misma computadora?.

De hecho, tu carpeta de Mis Documentos está normalmente visible para cualquiera, de modo que otros usuarios no tendrían siquiera que hacer algo inteligente para leer tus archivos no cifrados. Sin embargo, tienes razón, incluso si la

carpeta se hace 'privada,' todavía no estás a salvo a menos que utilices algún tipo de cifrado.

Consejos para utilizar el cifrado de archivos de manera segura

Almacenar datos confidenciales puede ser un riesgo para ti y para con quienes trabajas. El *cifrado* [48] reduce el riesgo pero no lo elimina. El primer paso para proteger información sensible es el reducir cuanto de ella mantienes a tu alrededor. A menos que tengas una buena razón para almacenar un archivo en particular, o una categoría particular de información dentro de un archivo, tú simplemente debes borrarla (dirígete al capítulo **6. Destruir información sensible** [80] para obtener mayor información de como hacerlo de manera segura.) El segundo paso es utilizar una buena herramienta de cifrado de archivos, tal como el *TrueCrypt* [77].

Claudia: Bien, tal vez no necesitamos en realidad almacenar información que podría identificar a las personas que nos dieron sus testimonios. ¿Qué opinas?

Pablo: De acuerdo. Probablemente deberíamos escribir lo menos posible sobre ello. Además, deberíamos pensar en un código simple que podamos utilizar para proteger los nombres y las ubicaciones que tenemos que registrar de todas maneras.

Regresando a la analogía de la caja fuerte cerrada, hay algunas cosas que debes tener en cuenta cuando utilices el *TrueCrypt* [77] u otras herramientas similares. No importa cuan robusta sea caja fuerte, no te hará mucho bien si dejas la puerta abierta. Cuando tu volumen TrueCrypt está 'montado' (el momento en que puedes acceder a su contenido), tus datos pueden ser vulnerables, de modo que debe mantenerse cerrado excepto cuando estás, ciertamente, leyendo o modificando los archivos dentro de este.

Existen algunas situaciones en las que es especialmente importante que recuerdes no dejar montado tu volumen *cifrado* [48]:

- Desconéctalo cuando debas alejarte de tu computadora por cualquier lapso de tiempo. Incluso si normalmente dejas tu computadora funcionando toda la noche, debes asegurarte de no dejar tus archivos sensibles accesibles a intrusos físicos o remotos mientras estás ausente.
- Desconéctalo antes de poner tu computadora a dormir. Esto se aplica a las opciones de 'suspendido' e 'hibernación', las cuales son comúnmente usadas con las computadoras portátiles pero que pueden estar presentes también en las computadoras de escritorio.
- Desconéctalo antes de permitir a alguien manejar tu computadora. Cuando pases tu computadora portátil a través de un control de seguridad o frontera, es importante que desconectes todos los volúmenes *cifrados* [48] y que apagues completamente tu computadora.
- Desconéctalo antes de insertar una memoria extraíble USB no confiable u otro dispositivo de almacenamiento externo, incluyendo aquellos que pertenezcan a tus amigos y colegas.
- Si mantienes un volumen *cifrado* [48] en una memoria extraíble USB, recuerda que el solo hecho de remover el dispositivo puede no desconectar inmediatamente el volumen. Incluso si necesitas mantener seguros tus archivos cuando estás apurado tienes que desmontar el volumen de forma apropiada, luego desconectar la unidad externa o la memoria extraíble, y luego retirar el dispositivo. Podrías desear practicar hasta que halles la forma más rápida de hacer todas estas cosas.

Si decides mantener tu volumen *TrueCrypt* [77] en una memoria extraíble USB, también puedes mantener una copia del programa TrueCrypt en ella. Esto te permitirá tener acceso a tus datos en las computadoras de otras personas. Sin embargo, las reglas normales todavía se aplican: si no confías en que la máquina esté libre de *software malicioso (malware)* [2], probablemente no deberías ingresar tus contraseñas o acceder a datos sensibles.

Ocultar tu información sensible

Un problema con el hecho de mantener una caja fuerte en tu casa u oficina, ni que decir de portarla, es que tiende a ser muy obvio. Muchas personas tienen preocupaciones razonables sobre autoincriminarse por medio del uso del *cifrado* [48]. Sólo porque las razones legítimas para cifrar datos exceden en número aquellas ilegítimas no hace esta amenaza menos real. Existen dos razones fundamentales por las que tú podrías evitar utilizar una herramienta como el *TrueCrypt* [81]: el riesgo de autoincriminación y el riesgo de identificar claramente la ubicación de tu información más sensible.

Considerar el riesgo de autoincriminación

El *cifrado* [48] es ilegal en algunos países, lo que significa que descargar, instalar o utilizar software de este tipo podría ser un crimen en si. Y, si la policía, el ejército o los servicios de inteligencia se hallan entre los grupos de quienes estás buscando proteger tu información, entonces el violar estas leyes puede proporcionarles un pretexto ideal bajo el cual tus

actividades pueden ser investigadas o tu organización perseguida. En realidad, amenazas como esta pueden no tener nada que ver con la legalidad de las herramientas en cuestión. En cualquier momento, el mero hecho de estar asociado con software de cifrado sería suficiente para exponerte a acusaciones de actividad criminal o espionaje—sin importar lo que realmente está dentro de los volúmenes cifrados-- por tanto debes pensar cuidadosamente respecto a si dichas herramientas son apropiadas o no para tu situación.

Si ese es el caso, tú tienes unas cuantas opciones:

- Puedes evitar completamente el utilizar software de seguridad de datos, lo que requerirá que almacenes información no confidencial o inventes un sistema de palabras códigos para proteger elementos clave de tus archivos sensibles.
- Puedes confiar en una técnica llamada *esteganografía* [82] para esconder tu información sensible, en vez de cifrarla. Existen herramientas que pueden ayudarte con ello, pero el utilizarlas adecuadamente requiere una preparación muy cuidadosa, y todavía corres el riesgo de incriminarte a los ojos de cualquiera que descubra que herramienta estás utilizando.
- Puedes intentar almacenar toda tu información sensible en una cuenta de correo electrónico con interfaz web segura, pero ello requiere de una conexión de red confiable y un relativamente sofisticado nivel de conocimiento de computadoras y de servicios de Internet. Esta técnica también asume que el *cifrado* [48] de red es menos incriminatorio que el cifrado de archivos y que no puedes evitar accidentalmente copiar datos sensibles en tu disco duro y dejarla ahí.
- Puedes mantener la información sensible lejos de tu computadora almacenándola en una memoria extraíble USB o en una disco duro portátil. Sin embargo, tales dispositivos son normalmente incluso más vulnerables que las computadoras a la perdida y a su confiscación, de modo que estar portando información sensible y no cifrada en uno de estos tipos de dispositivos es normalmente una mala idea.

Si es necesario, puedes emplear varias de estas tácticas. Sin embargo, incluso en circunstancias en las que estás preocupado sobre la autoincriminación, lo más seguro será utilizar el *TrueCrypt* [77], mientras tratas de camuflar tu volumen *cifrado* [48] de la mejor manera posible.

Si deseas que tu volumen cifrado sea menos llamativo, puedes renombrarlo para que se parezca a un tipo diferente de archivo. Utiliza la extensión '.iso', para camuflarlo como una imagen de CD, es una opción que funciona bien para grandes volúmenes de alrededor de 700 MB. Otras extensiones serían más realistas para pequeños volúmenes. Esto se asemeja a esconder tu caja fuerte detrás de una pintura en la pared de tu oficina. Este no será útil bajo inspección detallada, pero ofrecerá alguna protección. También puedes renombrar el mismo programa *TrueCrypt* [77], asumiendo que lo has guardado como harías con un archivo normal en tu disco duro o memoria extraíble USB, en vez de instalarlo como programa. La **guía del TrueCrypt** [81] te explica cómo hacerlo.

Considerar el riesgo de identificar tu información sensible

A menudo, debes preocuparte menos de las consecuencias de ser 'capturado' con software de *cifrado* [48] en tu computadora o en tu memoria extraíble USB y hacerlo más porque tu volumen cifrado indique específicamente donde almacenas la información que deseas proteger más. Aunque pueda ser cierto que nadie más pueda leerla, un intruso sabrá que está ahí, y que has dado pasos para protegerla. Ello te expone a varios métodos no técnicos a través de los cuales dicho intruso podría intentar tener acceso, ello incluye la intimidación, el chantaje, la interrogación y la tortura. Es en este contexto que la opción o característica de denegación del *TrueCrypt* [77], que se trata detalladamente más adelante, entra en juego.

La opción de denegación del *TrueCrypt* [77] es una de las maneras en las cuales este va más allá de lo ofrecido por las herramientas de *cifrado* [48] de archivos. Esta opción puede interpretarse como una forma peculiar de *esteganografía* [82] que disfraza tu información más sensible como otra, menos sensible, información oculta. Es análogo a instalar un astuto 'falso fondo' dentro de una no tan sútil caja fuerte. Si un intruso se roba tus llaves, o te intimida para que le des la combinación de la caja fuerte, este encontrará algún material de 'señuelo' convincente, pero no la información que realmente te importa proteger.

Sólo tú sabes que tu caja fuerte contiene un compartimiento oculto en su parte trasera. Esto te permite 'negar' que estás manteniendo algún secreto más allá de lo que ya le has dado al intruso, y podría ayudar a protegerte en situaciones en las cuales por alguna razón debes reveler una contraseña. Tales razones podrían incluir amenazas legales o físicas a tu propia seguridad, o aquella de tus colegas, asociados, amigos y familiares. El propósito de la denegación es el de darte una oportunidad de escapar de una situación potencialmente peligrosa incluso si decides continuar protegiendo tus datos. Sin embargo, como se trata en la sección de **Considerar el riesgo de la autoincriminación**, esta opción es mucho menos útil si el mero hecho de ser capturado con una caja fuerte en tu oficina es suficiente para provocar consecuencias inaceptables.

La opción de denegación del TrueCrypt funciona por medio del almacenamiento de un 'volumen oculto' dentro de un volumen común *cifrado* [48]. Este volumen oculto se abre proporcionando una contraseña alterna diferente a la que normalmente utilizarías. Incluso si un intruso técnicamente sofisticado logra acceder a tu volumen común, él será incapaz de probar que existe uno oculto. Por supuesto, el puede muy bien saber que el *TrueCrypt* [77] es capaz de ocultar información de esta forma, de modo que no hay garantía de que la amenaza desaparezca tan pronto como reveles tu contraseña señuelo. Muchas personas utilizan el TrueCrypt sin habilitar su opción de denegación, sin embargo, se considera en general que es imposible determinar, a través de un análisis, si un volumen cifrado contiene esta clase de 'falso fondo'. Eso nos dice, que es tu trabajo asegurarte de no revelar tu volumen oculto por medio de medios menos técnicos, tales como dejarlo abierto o permitir que otras aplicaciones creen accesos directos a los archivos que contiene.

La sección de **Lecturas Adicionales** [83], que viene a continuación, te puede dirigir a obtener mayor información al respecto.

Claudia: Bien, entonces vamos a arrojar algo de basura dentro del volumen común, y luego, podemos desplazar todos nuestros testimonios dentro del volumen oculto. ¿Tienes algunos viejos PDFs o algo que podamos utilizar?

Pablo: Justamente estuve pensando en ello, es decir, la idea es revelar la contraseña señuelo si no tenemos otra opción, ¿cierto? Pero para que ello sea convincente, necesitamos asegurarnos que dichos archivos se vean importantes, ¿no crees? De otro modo, ¿Por qué nos molestaríamos en cifrarlos? Tal vez deberíamos utilizar algunos documentos financieros no relacionados o una lista de contraseñas de sitios web o algo parecido.

Lecturas Adicionales

- Para información adicional sobre cómo asegurar tus archivos, dirígete al Capítulo de Criptología [84], y al Capítulo de Esteganografía [85] y al Caso de Estudio 3 [86] del libro de Seguridad Digital y Privacidad para Defensores de los Derechos Humanos [38] [1].
- La documentación sobre Truecrypt contiene en detalle aspectos sobre el cifrado de información y las Preguntas Frecuentes del TrueCrypt [87] [2] proporcionan respuestas a algunas preguntas comunes sobre el TrueCrypt.

Referencias

[1] www.frontlinedefenders.org/manual/en/esecman/ [30]
[2] www.truecrypt.org/faq.php [87]

5. Recuperar información perdida

Cada nuevo método de almacenamiento o transferencia de información digital tiende a introducir muchas más formas nuevas en las que la información en cuestión puede perderse, ser capturada o destruida. Años de trabajo pueden desaparecer en un instante, como resultado de un robo, un momento de descuido, la confiscación del hardware de la computadora, o simplemente debido a que la tecnología de almacenamiento es frágil por naturaleza. Existe un dicho común entre los profesionales dedicados al soporte técnico en el campo de la informática: "la cuestión no es *si* vas a perder tus datos; sino *cuando*." Por tanto, *cuando* esto te ocurra, es extremadamente importante que ya cuentes con un medio actualizado y probado de respaldo para poder restituir tus datos. Normalmente el día en que te recuerdan la importancia de un sistema de respaldo es al día siguiente que necesitaste tener uno en funcionamiento.

A pesar de ser uno de los elementos fundamentales de seguridad informática, el formular una política efectiva de mantenimiento de un respaldo no es tan simple como parece. Varios problemas se combinan para hacer de esto un obstáculo significativo, incluyendo la necesidad de almacenar datos originales y copias de seguridad o respaldos en diferentes ubicaciones físicas, la importancia de mantener confidenciales las copias de seguridad, y el reto de coordinar entre distintas personas quién comparte información con quién, utilizando sus propios dispositivos portátiles de almacenamiento. Además las copias de seguridad o respaldos y las tácticas de recuperación de archivos, este capítulo se ocupa de dos herramientas específicas, el *Cobian Backup* [88] y el *Undelete Plus* [89].

Contexto

Elena es una activista ecológica en un país de habla rusa, donde ha comenzado a crear un sitio web que dependerá de la presentación creativa de imágenes, videos, mapas y relatos que hagan hincapié en el grado de deforestación ilegal en la región. Ella ha estado recolectando por años documentos, archivos de medios de comunicación e información geográfica sobre la tala de árboles, y la mayoría de ellos están almacenados en una vieja computadora que funciona con Windows en la oficina de la ONG donde ella trabaja. Mientras estaba diseñando un sitio web con relación a esta información, se dio cuenta de la importancia de ésta y se empezó a preocupar sobre su resguardo en caso de que su computadora sea dañada, especialmente si esto ocurre antes de tenga todo copiado al sitio web. Otros miembros de su organización a veces utilizan la computadora, de modo que ella desea saber cómo restituir sus archivos si alguien accidentalmente borra la carpeta que contiene su trabajo. Ella le pide a su sobrino Nikolai que la ayude a elaborar una estrategia vinculada a la creación y mantenimiento de una copia de seguridad o respaldo.

¿Qué aprenderás en este capitulo?

- Cómo organizar y hacer un respaldo de tu información
- Dónde debes almacenar tus respaldos o copias de seguridad
- Cómo debes administrar de manera segura tus respaldos
- Cómo recuperar archivos que han sido accidentalmente borrados

Identificar y organizar tu información

Aunque es evidentemente importante que des pasos para evitar desastres — asegurándote que tu información está físicamente a salvo, libre de *software malicioso (malware)* [2] y protegido por un buen *cortafuegos (firewall)* [20] y contraseñas sólidas — eso no es suficiente. Simplemente existen demasiadas cosas que pueden salir mal, incluyendo ataques virales, *piratas informáticos (hackers)* [1], cortos circuitos, picos de tensión eléctrica, derrames de agua, robo, confiscación, desmagnetización, problemas con el sistema operativo, fallas de hardware, para nombrar unos cuantos. El prepararse para el desastre es tan importante como defenderse de este.

Elena: Sé que un respaldo es importante, Nikolai, pero eso no significa que ¿Debería tener a alguien más que lo configure para mi? Es decir, ¿Tendré el tiempo, recursos y experiencia para hacer esto por mi cuenta?

Nikolai: No te preocupes. El desarrollar un buen plan de creación de respaldo requiere un poco de reflexión, pero no toma mucho tiempo ni dinero. Y, comparado con perder toda tu información, muy difícilmente podrías llamarlo inconveniente, ¿correcto? Aparte de ello, el respaldo es definitivamente una de esas cosas que debes hacer tu mismo. A menos que la persona que te ayuda regularmente en la parte técnica sea extremadamente confiable y esté extremadamente informada sobre donde mantienes tu información digital, lo mejor es configurar las cosas por ti mismo.

El primer paso para formular una política para el respaldo es imaginar donde se halla actualmente localizada tu información personal y laboral. Tu correo electrónico - por ejemplo - puede estar almacenado en el servidor del proveedor de correo electrónico, en tu propia computadora, o en ambos lugares al mismo tiempo. Y, por supuesto, puedes tener muchas cuentas de correo electrónico. Además, existen importantes documentos en las computadoras que utilizas, las cuales pueden estar en la oficina como en tu domicilio. Hay agendas de direcciones, el historial de conversaciones y configuraciones personales de programas. También es posible que alguna información sea también almacenada en medios removibles, como memorias extraíbles USB, discos duros externos, CDs, DVDs, y viejos disquetes. Tu teléfono móvil tiene una lista de contactos y podría tener importantes mensajes de texto. Si tienes un sitio web, este podría contener una gran colección de artículos acumulados a lo largo de años de trabajo. Y, finalmente, no te olvides de tu información que no se halla en medios digitales, tales como agendas físicas, diarios y cartas.

Luego, necesitas definir cuales de estos archivos son 'copias maestras', y cuales son duplicados. La copia maestra es generalmente la versión más actualizada de un archivo en particular o una colección de archivos y corresponde a un archivo que en realidad editarás si necesitas actualizar su contenido. Obviamente esta distinción no se aplica a archivos de los cuales tienes una única copia, pero es extremadamente importante para ciertos tipos de información. Una situación común de desastre es cuando sólo los duplicados de cada documento importante son respaldados, y la copia maestra en sí se perdió o destruyó antes que estos duplicados pudieran ser actualizados. Imagina, por ejemplo, que has estado trabajando por una semana mientras actualizabas la copia de determinada hoja de cálculo que mantienes en tu memoria extraíble USB. A estas alturas, deberías empezar a pensar en aquella como tu copia maestra, debido a que los respaldos de la versión desactualizada que se hallan en la computadora de la oficina ya no son útiles.

Trata de anotar la ubicación física de todas tus copias maestras y de los duplicados de la información identificada anteriormente. Ello te ayudará a aclarar tus necesidades y empezar a definir una adecuada política de respaldos o copias de seguridad. El cuadro que hallamos a continuación es un ejemplo muy básico. Por supuesto, tu probablemente te percates que tu lista es mucho más extensa, y contiene algunos 'dispositivos de almacenamiento' con más de un 'tipo de dato' y algunos tipos de datos que se encuentran presentes en múltiples dispositivos.

Tipo de Datos	**Copia Maestra/Duplicado**	**Dispositivo de Almacenamiento**	**Ubicación**
Documentos electrónicos	Copia Maestra	Disco duro de la computadora	Oficina
Unos cuantos documentos electrónicos importantes	Duplicado	Memoria extraíble USB	Conmigo
Bases de datos de aplicaciones (fotos, agenda de direcciones, calendario, etc.)	Copia Maestra	Disco duro de la computadora	Oficina
Unos cuantos documentos electrónicos	Duplicado	CDs	Domicilio
Correo electrónico & contactos de correo electrónico	Copia Maestra	Cuenta de Gmail	Internet

Mensajes de texto & contactos telefónicos	Copia Maestra	Teléfono móvil	Conmigo
Documentos impresos (contratos, facturas, etc.)	Copia Maestra	Cajón de escritorio	Oficina

En el cuadro anterior, puedes apreciar que:

- Los únicos documentos que sobrevivirian si falla el disco duro de tu computadora de tu oficina son los duplicados en tu memoria extraíble USB y las copias en CD en tu domicilio.
- No tienes copias de tus mensajes de correo electrónico sin conexión o de tu agenda, de modo que si olvidas tu contraseña (o si alguien logra cambiarla maliciosamente), perderás acceso a ella.
- No tienes copias de ningún dato de tu teléfono móvil.
- No tienes duplicados, digitales o físicos, de documentos impresos tales como contratos y facturas.

Definir una estrategia para tu respaldo

Para hacer el respaldo de todos los datos listados anteriormente necesitarás una combinación de software y soluciones de proceso. Esencialmente debes asegurarte que cada tipo de datos sea almacenado en al menos dos lugares separados.

Documentos electrónicos - Crea el respaldo completo de todos los documentos en tu computadora utilizando un programa como el *Cobian Backup* [88], el cual se detalla más adelante. Almacena el respaldo en algún dispositivo portátil de modo que puedas llevarlo a tu domicilio o a cualquier otro lugar seguro. Los discos duros externos, CD's / DVD's o memorias extraíbles son opciones posibles. Algunas personas utilizan CDs o DVDs ya que es menor el riesgo de sobreescribir los documentos o perder los respaldos.Los CDs en blanco pueden ser lo suficientemente baratos de modo que puedas utilizar uno nuevo cada vez que hagas un respaldo. Debido a que este tipo de datos a menudo contienen la información más sensible, es particularmente importante que protejas los respaldos de tus documentos electrónicos utilizando algún tipo de cifrado. Puedes aprender cómo hacerlo en el capítulo **4. Proteger los archivos sensibles en tu computadora** [49] y en la **guía del TrueCrypt** [81].

Bases de datos de aplicaciones - Una vez que hayas determinado la ubicación de tus bases de datos de aplicaciones, puedes respaldarlas de la misma forma que los documentos electrónicos.

Correo electrónico - En vez de ingresar a tu correo electrónico sólo a través de un navegador web, instala un cliente de correo electrónico como el *Thunderbird* [26] y configúralo para funcionar con tu cuenta. La **guía del Thunderbird** [90] te explica en detalle cómo hacerlo. La mayoría de los servicios de correo con interfaz web te proporcionarán instrucciones de cómo utilizar dichos programas y - a menudo - cómo importar tu dirección de correo electrónico a éste. Puedes aprender más sobre esto en la sección Lecturas Adicionales que viene más adelante. Si decides mover tus mensajes de correo electrónico viejos a tu computadora para que no sean guardados en el servidor (por razones de seguridad por ejemplo), asegúrate de inlcuirlos en el respaldo electrónico de documentos como se describe arriba.

Contenidos de teléfono móvil - Para hacer un respaldo de los números telefónicos y mensajes de texto en tu teléfono móvil, puedes conectarlo a la computadora utilizando el software apropiado, el cual está normalmente disponible en el sitio web del fabricante de tu teléfono. Sin embargo, para esto puedes necesitar comprar un cable especial USB.

Documentos impresos - Cuando sea posible, debes escanear todos tus documentos importantes, luego respaldarlos junto con tus otros documentos electrónicos como se explicó anteriormente.

Al final debes haber dispuesto de manera diferente tus dispositivos de almacenamiento, tipos de datos y respaldos de manera que tu información sea más resistente al desastre:

Tipo de Datos	Copia Maestra/Duplicado	Dispositivo de Almacenamiento	Ubicación
Documentos electrónicos	Copia Maestra	Disco duro de la computadora	Oficina
Documentos electrónicos	Duplicado	CDs	Domicilio
Unos cuantos documentos electrónicos importantes	Duplicado	Memoria extraíble USB	Conmigo

Tipo de Datos	Copia Maestra/Duplicado	Dispositivo de Almacenamiento	Ubicación
Bases de datos de aplicaciones	Copia Maestra	Disco duro de la computadora	Oficina
Bases de datos de aplicaciones	Duplicado	CDs	Domicilio

Tipo de Datos	Copia Maestra/Duplicado	Dispositivo de Almacenamiento	Ubicación
Correo electrónico & contactos de			

Correo electrónico & contactos de correo electrónico	Duplicado	Cuenta Gmail	Internet
Correo electrónico y contactos de correo electrónico	Copia Maestra	Thunderbird en la computadora de la oficina	Oficina

Tipo de Datos	Copia Maestra/Duplicado	Dispositivo de Almacenamiento	Ubicación
Mensajes de texto y contactos en el teléfono móvil	Copia Maestra	Teléfono móvil	Conmigo
Mensajes de texto y contactos en el teléfono móvil	Duplicado	Disco duro de la computadora	Oficina
Mensajes de texto y contactos en el teléfono móvil	Duplicado	Respaldo de la tarjeta SIM	Domicilio

Tipo de Datos	Copia Maestra/Duplicado	Dispositivo de Almacenamiento	Ubicación
Documentos impresos	Copia Maestra	Cajón de escritorio	Oficina
Documentos escaneados	Duplicado	CDs	En casa

Elena: Sé de personas que guardan todos sus documentos importantes en Gmail, adjuntándolos a mensajes del tipo 'borrador' o correos electrónicos sí mismos. ¿Ello podría considerarse como una 'ubicación física secundaria' para mis archivos?

Nikolai: Te podría ayudar a recuperarlos si pierdes uno o dos documentos muy importantes, pero es muy raro. Sinceramente, ¿cuántos documentos por semana estarías dispuesto a respaldar de esa forma? Además, debes considerar si dichos archivos adjuntos están seguros o no, especialmente si estás preocupada sobre si tu correo electrónico está siendo monitoreado. A menos que estés conectada de manera segura al Gmail, esto es como entregar tu información sensible en una bandeja de plata. El utilizar una conexión HTTPS para Gmail con el fin de respaldar pequeños volúmenes de TrueCrypt o archivos de bases de datos de KeePass sería muy seguro, debido a que estos se hallan cifrados, pero yo no te recomendaría esto como objetivo general de tu estrategia de respaldos.

Crear un respaldo digital

De los distintos tipos de datos que se discuten aquí, los 'documentos electrónicos' son los que las personas tienden a preocuparse más cuando establecen una política de respaldo. Este término es algo ambiguo, pero generalmente se refiere a archivos de los cuales estás al tanto y que abres manualmente a través de una doble o utilizando algún programa en el menú de Archivo.Específicamente, incluye archivos de texto, documentos de procesador de textos, presentaciones, PDFs y hojas de cálculo, entre otros ejemplos. A diferencia de los mensajes de correo electrónico, por ejemplo, los documentos electrónicos generalmente no están sincronizados con copias remotas en la Internet.

Cuando hagas el respaldo de tus documentos electrónicos debes recordar también respaldar las bases de datos de tus aplicaciones. Si utilizas una aplicación de calendario o una agenda electrónica, por ejemplo, necesitarás encontrar las carpetas en las cuales estos programas almacenan sus datos. Con suerte estas bases de datos estarán en la misma ubicación de tus documentos electrónicos, ya que a menudo se mantienen dentro de la carpeta *Mis Documentos* en una computadora con Windows. Sin embargo, si ese no es el caso, debes añadir las carpetas pertinentes a tu respaldo normal.

Los correos electrónicos almacenados por una aplicación tal como el *Thunderbird* [26] es un ejemplo especial de un base de datos de aplicación. Si utilizas un programa de correo electrónico — y especialmente si no puedes o no deseas almacenar una copia de tus mensajes en el servidor — entonces debes de todas maneras asegurarte que esta base de datos de correo electrónico se incluya en tu respaldo normal. Puedes considerar a las imágenes y archivos de video como documentos electrónicos o elementos dentro de una base de datos de aplicación, eso depende de cómo interactúas con ellos. Las aplicaciones tales como el Windows Media Player y el iTunes, por ejemplo, funcionan como bases de datos. Si utilizas programas como estos, debes buscar en tu disco duro para saber donde se almacenan los archivos multimedia existentes que ayudan a administrar.

Dispositivos de almacenamiento

Antes de hacer un respaldo de tus documentos electrónicos, debes decidir qué tipo de dispositivo de almacenamiento usarás.

Memorias extraíbles USB - Estos dispositivos pueden ser baratos y ofrecer mayor capacidad de almacenamiento (memoria). Son fáciles de borrar o sobreescribir numerosas veces. Los USB tienen una vida útil, que depende en la forma o frecuencia de uso, pero se estima generalmente de 10 años.

Discos Compactos (CDs) - Los CDs almacenan alrededor de 700 Megabytes (MB) de datos. Para crear un respaldo en CD necesitarás un *quemador de CD* [91] y discos en blanco. Si deseas borrar un CD y actualizar los archivos almacenados en este, necesitarás tener un quemador de CD-RW y CDs regrabables. Todos los más difundidos sistemas operativos, incluyendo el Windows XP, ahora incluyen un software que puede grabar CDs y CD-RWs. Ten en cuenta que la información escrita en estos discos puede empezar a deteriorarse después de cinco o diez años. Si necesitas almacenar un respaldo por un tiempo mayor, tendrás que recrear ocasionalmente los CDs, comprar discos especiales de 'larga vida' o utilizar un método diferente de respaldo.

Discos Digitales de Video (DVDs) - Los DVDs almacenan hasta 4.7 Gigabytes (GB) de datos. Funcionan en forma parecida a los CDs pero necesitan un equipo ligeramente más costoso. Necesitarás un quemador de DVD o un *quemador de DVD-RW* [91], y discos apropiados. Del mismo modo como los CD, los datos escritos en un DVD normal eventualmente empezarán a desvanecer.

Servidor remoto - Un servidor de red de respaldo con buen mantenimiento puede tener una capacidad casi ilimitada, pero la velocidad y la estabilidad de tu propia conexión de Internet determinará si ésta es o no una opción realista. Ten en consideración que hacer un respaldo en un servidor en tu propia oficina, aunque más rápido que copiar información en la Internet, viola el requerimiento de mantener una copia de tus datos importantes en dos lugares físicos diferentes. Existen también servicios de almacenamiento gratuito en la Internet, pero siempre debes cifrar tus respaldos antes de subirlos a servidores a cargo de organizaciones o individuos a quiénes no conoces ni en quiénes confias. Dirígete a la sección **Lecturas Adicionales** [92] para ver algunos ejemplos.

Software para hacer respaldos

El *Cobian Backup* [88] es una herramienta de fácil manejo que puede configurarse para funcionar automáticamente en periodos predeterminados, y para incluir sólo los archivos que han sido modificados desde la última creación de respaldo. Este también puede comprimir respaldos para hacerlos más pequeños.

Parte Práctica: Empieza con la Guía del Cobian Backup [93]

Como siempre, es una buena idea cifrar tus archivos de respaldo utilizando una herramienta como el *TrueCrypt* [77]. Más información sobre el cifrado de datos puede hallarse en el capítulo **4. Proteger los archivos sensibles en tu computadora** [49].

Parte Práctica: Empieza con la Guía del TrueCrypt [81]

Cuando estés utilizando estas herramientas para hacer respaldos, hay algunas cosas que puedes hacer para ayudar que el sistema de respaldo trabaje sin problemas:

- Organiza los archivos en tu computadora. Trata de trasladar todas las carpetas que contienen documentos electrónicos que intentas respaldar a un solo lugar, tal como la carpeta **Mis Documentos**.
- Si utilizas un software que almacena sus datos en una base de datos de aplicación, debes primero determinar la ubicación de dicha base de datos. Si no está en un lugar conveniente, infórmate si el programa te permite elegir una nueva ubicación para su base de datos. Si es posible, puedes colocar esta en la misma carpeta de tus documentos electrónicos.
- Crea un horario regular para hacer tu respaldo.
- Trata de establecer procedimientos para todo el personal en tu oficina que todavia no tiene una política confiable y segura de respaldos. Ayuda a tus compañeros/as de trabajo a entender la importancia de este tema.
- Asegúrate de probar el proceso de recuperación de datos de tu respaldo o copia de seguridad. Recuerda, que al final, ¡es el proceso de restitución — no el procedimiento de respaldo — el que de veras te importa!

Elena: Está bien, hice un respaldo cifrado mientras estaba en el trabajo, y lo grabé en un CD. El Cobian está programado para actualizar mi respaldo en unos cuantos días. Mi escritorio en el trabajo tiene un cajón con cerradura, y estoy pensando mantener los CDs de respaldo en este de modo que no se pierdan o rompan.

Nikolai: ¿Qué sucedería si tu oficina se incendia? ¿La computadora, el escritorio, los CDs de respaldo y todo lo demás? O, ¿Qué ocurriría si tu sitio web es utilizado para planificar una gran manifestación ambientalista, las autoridades los combaten, las cosas se salen de las manos y la organización es allanada? Dudo mucho que tu pequeño candado del escritorio detenga a la policía de confiscar esos CDs. ¿Por qué no guardarlos en tu casa, o pedir a un amigo que te los

guarde ?

Recuperarse de un borrado accidental de archivos

Cuando borras un archivo en Windows, este desaparece de la vista, pero sus contenidos se mantienen en la computadora. Incluso después de que hayas vaciado tu Papelera de Reciclaje, la información de los archivos que has borrado pueden normalmente ser ubicados en el disco duro. Dirígete al capítulo **6. Destruir información sensible** [80] para aprender más sobre esto. De vez en cuando, si accidentalmente borras un archivo o carpeta importante, esta vulnerabilidad de seguridad puede trabajar a tu favor. Existen numerosos programas que pueden restituir el acceso a tus recientemente borrados archivos, incluyendo un herramienta *Recuva*.

Parte Práctica: Empieza con la Guía del Recuva [94]

Estas herramientas no siempre funcionan, debido a que Windows pudo haber escrito nuevos datos sobre tu información borrada. Por tanto es importante que utilices lo menos posible tu computadora en el tiempo entre el borrado del archivo y el intento de restituirlo con una herramienta como *Recuva*. Cuanto más tiempo utilices tu computadora antes de intentar recuperar el archivo, será menos probable que tengas éxito. Esto también significa que debes utilizar la versión portable de Recuva en lugar de instalarlo después de borrar un archivo importante. Instalar el programa requiere que escribas información nueva en el archivo del sistema, lo que coincidentemente sobreescribirá encima de los datos críticos que estás tratando de recuperar.

Aunque puede parecer mucho trabajo el implementar las políticas y aprender a utilizar las herramientas descritas en este capítulo, el mantener tu estrategia de respaldo, una vez que tengas un sistema en pie, es mucho más fácil que configurarla por primera vez. Y dado que el respaldo puede ser el aspecto individual más importante de la seguridad de datos, puedes estar seguro que el esfuerzo de recorrer todo el proceso bien vale la pena.

Lecturas Adicionales

- Mayor información sobre el respaldo y la recuperación de datos puede hallarse en Respaldo, Destrucción y Recuperación de Información [95] capítulo del libro Seguridad Digital y Privacidad para Defensores de los Derecho Humanos [30] [1].
- Note que realizar respaldos en línea implica nuevos riesgos. Como mínimo recuerde cifrar tu información sensible y de forma separada tu mismo/a antes de subirlo al servidor. Asumiendo que haces el paso anterior, existen servicios gratuitos de almacenamiento en línea que te proporcionan una forma conveniente de respaldo de tu información. Algunas opciones son Wuala [96] [2], SpiderOak [97] [3], Google Drive [98] [4], tahoe-lafs [99] [5].
- Existe un excelente artículo sobre recuperación de datos en Wikipedia [100] [6].

Referencias

[1] www.frontlinedefenders.org/manual/en/esecman [38]
[2] https://www.wuala.com [101]
[3] https://spideroak.com [102]
[4] https://drive.google.com/start [103]
[5] https://tahoe-lafs.org/trac/tahoe-lafs [104]
[6] www.en.wikipedia.org/wiki/Data_recovery [105]

6. Destruir información sensible

Los capítulos anteriores se han ocupado de varias herramientas y hábitos que pueden ayudarte a proteger tus datos sensibles, pero ¿Qué ocurre cuando decides que ya no necesitas más conservar una parte de tu información? Si determinas, por ejemplo, que tus copias cifradas de respaldo de un archivo en particular son suficientes, y deseas borrar la copia maestra, ¿Cuál es la mejor forma de hacerlo? Lamentablemente, la respuesta es más complicada de lo que crees. Cuando borras un archivo, incluso antes de vaciar la **Papelera de Reciclaje**, los contenidos de dicho archivo se mantienen en tu disco duro y pueden ser recuperados por cualquiera que tenga un poco de suerte y las herramientas adecuadas.

Con el fin de garantizar que la información borrada no termine en las manos equivocadas tendrás que confiar en un software especial que remueva los datos de manera segura y permanente. El *Eraser* [106] es una de tales herramientas, y se abordará más adelante. Utilizar el Eraser es un poco como hacer trizas un documento de papel en vez de simplemente arrojarlo dentro de una papelera y esperar que nadie lo encuentre. Y, por supuesto, el borrar archivos es solo un ejemplo de una situación en la cual podrías necesitar destruir datos sensibles. Si consideras los detalles que alguien, particularmente un adversario poderoso y motivado políticamente, podría descubrir sobre ti o tu organización al leer ciertos archivos que pensaste que habías borrado, podrías probablemente pensar en algunos cuantos ejemplos más: destruir respaldos obsoletos, *eliminar permanentemente* [107] los datos de viejos disco duros antes de regalarlos, borrar viejas cuentas de usuario, y limpiar tu historial de navegación, para mencionar unos cuantos. La otra herramienta descrita en este capitulo es el *CCleaner* [108], que te puede ayudar a afrontar el reto de borrar los muchos archivos temporales que tu sistema operativo y las aplicaciones crean cada vez que los usas.

Contexto

Elena es una activista medioambiental en un país de habla rusa, donde mantiene un crecientemente popular sitio web que hace hincapié en la magnitud de la deforestación ilegal en la región. Ella ha creado un respaldo de la información utilizada para crear el sitio web, y mantiene copias de este en casa, en la oficina y en su nueva computadora portátil. Hace poco, ha empezado a almacenar copias de los registros de visita de los servidores web y de la base de datos que contiene sus mensajes en el foro de usuarios. Elena pronto hará un viaje internacional, para asistir a una gran conferencia mundial de activistas medioambientales, algunos de los cuales han informado que sus computadoras portátiles les fueron quitadas por aproximadamente una hora en los pasos fronterizos. Para proteger su información sensible, y la seguridad de los participantes más políticos de su foro, ella ha trasladado sus respaldos de casa y de la oficina a un volumen TrueCrypt y ha removido la copia que había en su computadora portátil. Le pidió consejo a su sobrino Nikolai, y él le advirtió que tiene que hacer algo más que sólo borrar su viejo respaldo si le preocupa la retención de su computadora a cargo de los funcionarios de fronteras.

¿Qué puedes aprender de este capítulo?

- Eliminar de manera permanente información sensible de tu computadora
- Eliminar información almacenada en tus dispositivos de almacenamiento removibles tales como CDs y memorias extraíbles USB
- Evitar que alguien sepa que documentos has estado viendo previamente en tu computadora
- Mantener tu computadora de modo que los archivos borrados no puedan ser recuperados en el futuro

Borrar información

Desde una perspectiva puramente técnica no existe en tu computadora una función de borrado propiamente dicha. Por supuesto puedes arrastrar un archivo a la **Papelera de Reciclaje** y vaciarla, pero todo esto en realidad simplemente borra el icono, elimina el nombre del archivo de una especie de índice de todo el contenido en tu computadora y le dice a Windows que puede utilizar ese espacio para algo más. Sin embargo, hasta que esto ocurra dicho espacio será ocupado por los contenidos de la información borrada, algo muy parecido a un gabinete de archivos al que se le ha sacado todas sus etiquetas pero todavía contiene todos los archivos originales. Es por esto que si cuentas con el software adecuado y actúas con prisa, puedes recuperar la información que borraste por accidente, como se trató en el capítulo **5. Recuperar información perdida** [52].

Debes tener en cuenta que cada vez que usas tu computadora, se crean archivos y estos mismos son borrados de manera insegura, sin tu conocimiento. Supón, por ejemplo, que estás escribiendo un informe extenso. Este te podría tomar una semana, trabajando muchas horas a diario, y cada vez que el documento es guardado, Windows creará una nueva copia del documento y lo almacenará en tu disco duro. Después de unos cuantos días de editado, tú puedes sin saberlo haber guardado muchas versiones del documento, todas en diferentes etapas de avance.

Por supuesto, Windows generalmente borra las versiones antiguas de un archivo, pero no busca la ubicación exacta del original para sobrescribirlo de manera segura cuando se hace una nueva copia. En vez de ello, este simplemente pone la última versión en una nueva sección del hipotético gabinete de archivos mencionado anteriormente, es decir, traslada la etiqueta de la vieja sección a la nueva, y deja el anterior borrador donde estaba hasta que otro programa requiera utilizar ese espacio. Está claro, que si tú tienes una buena razón para destruir todos los rastros de dicho documento de tu gabinete de archivos, el borrar la última copia no será suficiente, y simplemente el botar la etiqueta sería mucho peor.

También debes recordar, que los discos duros de la computadora no son los únicos dispositivos que almacenan información digital. Los CDs, DVDs., las memorias extraíbles USB, los disquetes, las tarjetas de memoria flash de los teléfonos móviles y los discos duros externos tienen los mismos problemas, y no debes confiar simplemente en una simple operación de borrar o reescribir para desaparecer información sensible de cualquiera de ellos.

Eliminar permanentemente información con herramientas seguras de borrado

Cuando utilizas una herramienta de borrado seguro - tal como aquellas recomendadas en este capitulo - sería más preciso decir que estás reemplazando, o 'sobrescribiendo', tu información sensible, en vez de simplemente borrarla. Si imaginas que dichos documentos, en el gabinete de archivos deficientemente etiquetado que mencionamos antes, están escritos a lápiz, entonces un software de borrado seguro no sólo borra el contenido, sino que garabatea sobre cada palabra. Y - en forma muy parecida al trazo de la mina de un lápiz - la información digital puede todavía leerse, aunque con dificultad, incluso después de que ha sido borrada y se ha escrito algo sobre ella. Debido a esto las herramientas recomendadas aquí sobrescriben archivos múltiples veces con datos aleatorios. A este proceso se le llama *eliminar permanentemente* [107], y cuantas más veces es sobrescrita la información, mayor es la dificultad para que alguien pueda recuperar el contenido original. Los expertos coinciden generalmente que tres o más pasadas deben hacerse — algunos estándares recomiendan siete o más — pero el software de eliminación permanente de datos se ocupa de esto automáticamente.

Eliminar permanentemente archivos

Existen dos maneras comunes de *eliminar permanentemente* [107] datos sensibles de tu disco duro o de tu dispositivo de almacenamiento. Puedes eliminar permanentemente un archivo o puedes eliminar permanentemente todo el espacio 'no asignado' en la unidad. Cuando tomes esta decisión, puede ser útil considerar nuestro ejemplo previo del extenso informe que haya podido dejar copias incompletas esparcidas en todo tu disco duro aunque sólo un archivo es visible. Si eliminas permanentemente el archivo mismo, garantizas que la actual versión esta completamente removida, pero dejas las otras copias donde esten. De hecho, no existe manera de apuntar directamente a dichas copias, debido a que ellas no están visibles sin utilizar un software especial. Sin embargo, al eliminar permanentemente todo el espacio en blanco de tu dispositivo de almacenamiento, te aseguras que toda la información anteriormente borrada sea destruida. Regresando a la metáfora del gabinete de archivos, este procedimiento es comparable a buscar en el gabinete, borrar y garabatear sobre cada documento cuya etiqueta haya sido retirada.

El *Eraser* [106] es una herramienta de borrado segura, libre y de código abierto, que es extremadamente fácil de usar. Con el Eraser puedes *eliminar permanentemente* [107] archivos en tres diferentes formas: seleccionando un solo archivo, seleccionando el contenido de la **Papelera de Reciclaje**, o eliminando permanentemente todo el espacio no asignado en la unidad. El Eraser puede también eliminar permanentemente los contenidos del *archivo de paginación o intercambio* [109] de Windows, como se abordó anteriormente.

Parte Práctica: Empieza con la Guía del Eraser [110]

Aunque las herramientas de borrado seguro no dañarán ningún archivo visible a menos que tú expresamente los elimines permanentemente, es importante ser cuidadoso con un software como este. Después de todo los accidentes ocurren, es por ello que la gente considera muy útiles a la **Papelera de Reciclaje** y a las herramientas de recuperación de datos. Si te acostumbras a *eliminar permanentemente* [107] tus datos cada vez que borras algo, te encontraras sin forma de recuperarte de un simple error. Asegúrate siempre de tener un respaldo seguro antes de eliminar permanentemente grandes cantidades de datos de tu computadora.

Elena: Sé que los programas de procesamiento de textos como Microsoft Word y Open Office a veces realizan copias temporales de archivos mientras estás trabajando en ellos. Existen otros programas que hagan lo mismo, o ¿debo solamente preocuparme en mayor parte sobre los archivos que yo he creado y borrado?

Nikolai: En realidad, existen muchos lugares en tu computadora donde los programas dejan rastros de tu información personal y de tus actividades en línea. Te hablo de los sitios web que has visitado, los borradores de correos electrónicos que has escrito recientemente y otras cosas parecidas. Todo esto podría ser sensible, dependiendo de cuan a menudo utilizas esa computadora.

Eliminar permanentemente datos temporales

La opción que permite al *Eraser* [106] *eliminar permanentemente* [107] todo el espacio no asignado de una unidad no es tan riesgoso como parece, debido a que sólo elimina permanentemente contenido borrado anteriormente. Los archivos

visibles normalmente no serán afectados. Por otro lado, este mismo hecho sirve para resaltar un aspecto diferente: el Eraser no puede ayudarte a limpiar la información sensible que no ha sido borrada pero que pudiera estar extremadamente bien oculta. Los archivos que contienen dichos datos pueden estar metidos en carpetas oscuras, por ejemplo, o almacenados con nombres sin significado. Este no es un gran problema para documentos electrónicos, pero puede ser importante para información que se recolecta automáticamente cada vez que utilizas tu computadora. Ejemplos de ello incluyen:

- Datos temporales registrados por tu navegador mientras te muestra páginas web, incluyendo texto, imágenes, *cookies* [111], información de cuenta, datos personales utilizados para llenar formularios en línea y el historial de sitios web visitados.
- Archivos temporales guardados por varias aplicaciones con el fin de ayudarte a recobrarlos en caso se cuelgue tu computadora antes de que guardes tu trabajo. Estos archivos pueden contener texto, imágenes, datos de hojas de cálculo y los nombres de otros archivos, entre otra información potencialmente sensible.
- Archivos y enlaces almacenados por Windows en nombre de la conveniencia, tales como accesos directos a aplicaciones que has utilizado recientemente, enlaces obvios a carpetas que preferirías ocultas y, por supuesto, los contenidos de tu **Papelera de Reciclaje** que olvidaste vaciar.
- El *archivo de paginación o de intercambio* [109] de Windows. Cuando la memoria de tu computadora está llena, como cuando has estado ejecutando muchos programas al mismo tiempo en una vieja computadora, Windows a veces copia los datos que estás utilizando en un archivo extenso llamado archivo de paginación o de intercambio. Como resultado de ello este archivo puede contener casi todo, incluyendo las páginas web, los contenidos de los documentos, las contraseñas o las claves de cifrado. Incluso cuando apagas tu computadora, el archivo de paginación o intercambio no se remueve, por ello debes *eliminarlo permanentemente* [107] de forma manual.

Con el fin de remover archivos temporales comunes de tu computadora, puedes utilizar la herramienta de software libre llamada *CCleaner* [108], la cual fue diseñada para realizar la limpieza después de utilizar programas como el Internet Explorer, Mozilla *Firefox* [16] y las aplicaciones de Microsoft Office — todas las cuales son conocidas por exponer información potencialmente sensible — así como el mismo Windows. El CCleaner puede borrar archivos de forma segura, lo cual te ahorra el tener que *eliminar permanentemente* [107] el espacio no asignado de la unidad, usando el *Eraser* [106], después de utilizarlo.

Parte Práctica: Empieza con la Guía del CCleaner [112]

Consejos para utilizar de manera efectiva las herramientas seguras de borrado

Ahora que estás familiarizado con algunas de las formas en las cuales la información puede ser expuesta en tu computadora o en un dispositivo de almacenamiento, incluso si eres diligente en cuanto al borrado de archivos sensibles. También sabes que herramientas puedes utilizar para *eliminar permanentemente* [107] dicha información en forma permanente. Existen unos cuantos pasos simples que debes seguir, especialmente si es la primera vez que estás utilizando estas herramientas, con el fin de garantizar que tu unidad sea limpiada de manera segura y efectiva:

- Crea un respaldo cifrado de tus archivos más importantes, como se trató en el capítulo **5. Recuperar información perdida** [52]**.**
- Cierra todos los programas innecesarios y desconéctate de Internet.
- Borra todos los archivos innecesarios, de todos los dispositivos de almacenamiento, y vacía la *Papelera de Reciclaje*.
- *Elimina permanentemente* [107] los archivos temporales utilizando el *CCleaner* [108].
- Elimina permanentemente el *archivo de paginación o de intercambio* [109] de Windows utilizando el *Eraser* [106].
- Elimina permanentemente todo el espacio libre de tu computadora y de otros dispositivos de almacenamiento utilizando el Eraser. Podrías necesitar que este procedimiento se ejecute en la noche, pues puede ser muy lento.

Luego, debes habituarte a:

- Utilizar periódicamente el *CCleaner* [108] para *eliminar permanentemente* [107] tus archivos temporales
- *Eliminar permanentemente* los documentos electrónicos sensibles utilizando el *Eraser* [106], en vez de utilizar la *Papelera de Reciclaje* o la función de borrado de Windows
- Utilizar periódicamente el Eraser para eliminar permanentemente el archivo de paginación o de intercambio de Windows
- Utilizar periódicamente el Eraser para eliminar permanentemente todo el espacio no asignado en tus discos duros, memorias extraíbles USB, y cualquier otro dispositivo de almacenamiento que pudiera tener información sensible borrada recientemente. Entre ellos se puede incluir disquetes, CDs regrabables, DVDs regrabables y tarjetas de

memoria flash de cámaras, teléfonos móviles o reproductores portátiles de música.

Consejos para eliminar permanentemente el contenido completo de un dispositivo de almacenamiento

Podrías ocasionalmente necesitar *eliminar permanentemente* [107] los contenidos de un dispositivo de almacenamiento. Cuando vendes o regalas una vieja computadora, lo mejor es retirar el disco duro y que el nuevo dueño de la computadora adquiera una para sí. Sin embargo, si esta no es una opción, debes al menos eliminar permanentemente los contenidos del disco de manera rigurosa con el *Eraser* [106] antes de entregarlo. Incluso en el caso en el que conserves el disco, probablemente quieras eliminar permanentemente de todas maneras su contenido, sin importar si pretendes reutilizarlo o desecharlo. De manera similar si compras un nuevo disco duro, debes eliminar permanentemente los contenidos del antiguo después de copiar tus datos y hacer un respaldo seguro de este. Si lo que pretendes es botar o reciclar un viejo disco duro, también debes considerar el destruirlo físicamente. (Muchos profesionales a cargo del mantenimiento de las computadoras recomiendan unos cuantos golpes fuertes con un martillo antes de desechar cualquier dispositivo de almacenamiento que alguna vez contuvo información sensible.)

En cualquiera de las situaciones descritas anteriormente, necesitarás utilizar el *Eraser* [106] para *eliminar permanentemente* [107] el contenido total de un disco duro, lo cual es imposible mientras el sistema operativo se este ejecutando en ese disco en particular. La manera más fácil de tratar este asunto es remover el disco y colocarlo en una 'cubierta de disco' externa USB la cual puedes luego conectar a cualquier computadora que tenga instalado el Eraser. En este punto, puedes borrar el contenido completo del disco externo y luego utilizar el Eraser para eliminar permanentemente todo su espacio no asignado. Afortunadamente, esto no es algo que tengas que hacer a menudo, pues puede tomar un buen periodo de tiempo.

En vez de *eliminar permanentemente* [107] los datos que han sido almacenados en un CD o DVD regrabable, es mejor destruir el disco mismo. Si es necesario, puedes crear uno nuevo que contenga cualquier información que desees mantener. Y, por supuesto, esta es la única manera de 'borrar' el contenido de un disco no regrabable. Es sorprendentemente difícil destruir completamente los contenidos de un CD o DVD. Seguramente has escuchado historias sobre información recuperada de tales discos incluso después de que fueran cortados en pequeños pedazos. Aunque estas historias son ciertas, el reconstruir la información de esta manera toma mucho tiempo y pericia. Debes juzgar por ti mismo si es probable o no que alguien gaste ese nivel de recursos con el fin de acceder a tus datos. Normalmente, un par de fuertes tijeras o una fuerte cortadora de papel hará un buen trabajo. Si deseas tomar precauciones adicionales, puedes mezclar las piezas resultantes y disponer de ellas en varias ubicaciones alejadas de tu casa u oficina.

Elena: Todavía tengo un viejo CD de respaldo de los registros del servidor web, y escuché que puedes borrar un CD colocándolo en el microondas. Sin embargo, esto me suena a una mala idea. ¿Las personas en realidad hacen esto? ¿Realmente funciona?

Nikolai: Me imagino que destruye los datos de manera muy efectiva, pero no podría saberlo, porque ¡nunca pondría un CD en un microondas! Estás en lo correcto. Eso suena como una muy mala idea. Incluso si el metal no daña tu microondas o inicia un incendio, te apuesto que el plástico emitirá humos muy insalubres. Pensando en ello, no recomendaría tampoco el someter CDs al fuego.

Lecturas Adicionales

- Aunque no utiliza técnicas de borrado seguro para eliminarlos permanentemente, el Mozilla Firefox tiene incorporada una manera de borrar muchos de sus archivos temporales. Esta característica se describe en la Sección de la **Guía del Firefox** [113] y en el sitio web del Mozilla Firefox [114] [1].
- La sección de Preguntas Frecuentes del CCleaner [115] [2] proporciona información adicional sobre la instalación y el uso de esta herramienta
- Aunque la mayor parte del ensayo es muy técnico, la introducción de Peter Guttmann de su Borrado Seguro de Datos de Memorias Magnéticas y Transistorizadas [116] [3] vale la pena ser leído, pues el método [117] [4] que describe ha tenido una gran influencia en los desarrolladores del Eraser y de otras herramientas de remoción segura de archivos.

Referencias

[1] http://support.mozilla.com/en-US/kb/Clearing+Private+Data [114]
[2] www.ccleaner.com/help/faq [115]
[3] www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann [118]
[4] www.en.wikipedia.org/wiki/Gutmann_method [117]

7. Mantener privada tu comunicación en Internet

La conveniencia, la relación costo-beneficio y la flexibilidad del correo electrónico y de la mensajería instantánea los hace extremadamente valiosos para las personas y las organizaciones, incluso para aquellas con el acceso más limitado a la Internet. Para aquellos con conexiones más rápidas y más confiables, programas como Jitsi, *Skype* [43] y otras herramientas de *Voz sobre Protocolo de Internet (VoIP)* [119] también comparten estas características. Lamentablemente, estas alternativas digitales a los medios tradicionales de comunicación no siempre pueden ser confiables para mantener privada información sensible. Por supuesto, esto no es nada nuevo. El correo postal, las llamadas telefónicas y los mensajes de texto también son vulnerables, particularmente cuando se utilizan por quienes son objeto de vigilancia por parte de las autoridades.

Una diferencia importante entre las comunicaciones digitales, métodos de comunicación basados en Internet y métodos más tradicionales, es que la primera a menudo te permite elegir tu propio nivel de seguridad. Si envías correos electrónicos, mensajes instantáneos y conversaciones en *Voz sobre Protocolo de Internet (VoIP)* [119] utilizando métodos inseguros, éstos son casi con certeza menos privados que las cartas físicas o las llamadas telefónicas. Esto ocurre, en parte, debido a que algunas muy poderosas computadoras pueden automáticamente buscar a través de grandes cantidades de información digital para identificar a los remitentes, los destinatarios y palabras claves específicas. Se requieren de grandes recursos para llevar a cabo el mismo nivel de vigilancia para canales de comunicación tradicionales. Sin embargo, si tomas ciertas precauciones, puedes hacer realidad lo opuesto. La flexibilidad de las herramientas de comunicación de Internet y la fortaleza del *cifrado* *[48]* moderno pueden ahora proporcionarnos un nivel de privacidad que alguna vez sólo estuvo al alcance de los ejércitos nacionales y de las organizaciones de inteligencia.

El seguir las guías y explorar el software que se trata en este capítulo, puedes mejorar enormemente la seguridad de tus comunicaciones. El servicios de correo electrónico *Riseup* [120], el complemento *OTR* [121] para el programa de mensajería instantánea de *Pidgin* [122], el Mozilla *Firefox* [16] y el complemento *Enigmail* [123] para el cliente de correo electrónico Mozilla *Thunderbird* [26] son todas excelentes herramientas. Sin embargo, cuando las utilices debes tener en cuenta que la privacidad de una conversación nunca estará cien por ciento garantizada. Siempre existe alguna amenaza que no has considerado, ya sea un *registrador de teclas (keylogger)* [124] en tu computadora, una persona escuchando tras la puerta, un corresponsal de correo electrónico descuidado o algo completamente diferente. El objetivo de este capítulo es ayudarte a reducir incluso las amenazas que note ocurren, mientras evitamos la posición extrema, favorecida por algunos, de que no debes enviar nada por internet que no estés dispuesto/a a comunicar públicamente.

Contexto

Claudia y Pablo trabajan con una ONG de derechos humanos en un país sudamericano. Después de pasar varios meses recolectando testimonios de testigos de violaciones de derechos humanos que fueron cometidos por miembros del ejército en su región, Claudia y Pablo han empezado a dar pasos para proteger los datos resultantes. Ellos mantienen sólo la información que necesitan, la cual almacenan en una partición TrueCrypt que está respaldada en varias ubicaciones físicas. Mientras se preparan para publicar ciertos aspectos de estos testimonios en un próximo informe, ellos se han percatado que deben debatir información sensible con unos cuantos de sus colegas en otro país. Aunque han acordado no mencionar nombres ni ubicaciones, aún así quieren garantizar que sus correos electrónicos y conversaciones a través de mensajería instantánea sobre este tema se mantengan privadas. Después de convocar a una reunión para ocuparse de la importancia de la seguridad en la comunicación, Claudia pregunta si alguien en la oficina tiene alguna inquietud.

¿Qué puedes aprender de este capítulo?

- Porqué la mayoría de los correos con interfase web y servicios de mensajería instantánea no son seguros.
- Cómo crear una nueva y más segura cuenta de correo electrónico.
- Cómo mejorar la seguridad en tu actual cuenta de correo electrónico.
- Cómo utilizar un servicio seguro de mensajería instantánea.
- Qué hacer en caso que sospeches que alguien podría estar accediendo a tu correo electrónico.
- Cómo verificar la identidad de un corresponsal de correo electrónico.

Asegurar tu correo electrónico

Existen pocos pasos importantes que puedes dar para incrementar la seguridad de tu comunicación por correo electrónico. El primero es asegurarte que sólo la persona a quien le envías el mensaje sea capaz de leerlo. Esto se trata en las secciones **Mantener privado tu correo con interfaz web** y **Cambiarse a una cuenta de correo electrónico más segura**, que vienen a continuación.

Yendo más allá de los fundamentos, a veces es crítico que tus contactos de correo electrónico tengan la capacidad de verificar, sin duda, que un mensaje en particular efectivamente viene de ti y no de alguien que podría estar intentando hacerse pasar por ti. Una manera de lograrlo está en la sección **Seguridad avanzada de correo electrónico** [125], dentro de la sección **Cifrar y autenticar los mensajes individuales** [126].

También debes saber qué hacer si sospechas que la privacidad de tu cuenta de correo electrónico ha sido violada. La sección **Consejos para responder a una sospecha de violación de correo electrónico** [127] se ocupa de esta interrogante.

Recuerda, también que el asegurar el correo electrónico no tendrá ningún efecto positivo si todo lo que ingresas se registra por medio de un software espía (spyware) y es enviado de manera periódica por medio de la Internet a un tercero. El capítulo **1. Proteger tu computadora de software malicioso (malware) y piratas informáticos (hackers)** [128] ofrece algunos consejos sobre como evitar esta clase de cosas, y el capítulo **3. Crear y mantener contraseñas seguras** [129] te ayudará a proteger tus cuentas para el correo electrónico y las herramientas de mensajería instantánea descritas a continuación.

Mantener privado tu correo con interfaz web

La Internet es una red abierta a través de la cual la información normalmente viaja en formato legible. Si un mensaje común de correo electrónico es interceptado en su ruta hacia el destinatario, su contenido puede ser leído muy fácilmente. Y, debido a que la Internet es una gran red que depende de computadoras intermedias para dirigir el tráfico, muchas personas distintas pueden tener la oportunidad de interceptar un mensaje de esta manera. Tu *Proveedor de Servicio de Internet (ISP)* [130] es el primer destinatario de un mensaje de correo electrónico cuando este inicia su viaje hacia el destinatario final. De manera similar, el ISP del destinatario es la última parada para tu mensaje antes de ser entregado. A menos que tomes ciertas precauciones, tus mensajes pueden ser leídos o interferidos en cualquiera de estos puntos, o mientras viaja.

Pablo: Estuve hablando con uno de nuestros colegas acerca de todo esto, y ella dijo que ella y sus colegas a veces simplemente guardan mensajes importantes en la carpeta de 'Borradores' de su cuenta de correo con interfaz web donde todos comparten una contraseña. Esto me suena un tanto extraño, pero ¿Funciona? Es decir, ¿ese hecho no evitaría que alguien lea los mensajes, ya que en realidad nunca los enviaron?

Claudia: Sea cual fuera el momento en que lees un mensaje de correo electrónico en tu computadora, incluso si es solamente un 'borrador', su contenido ha sido enviado a ti a través de la Internet. De lo contrario, no podría aparecer en tu pantalla ¿correcto? La cosa es que si alguien te tiene bajo vigilancia, ellos simplemente no vigilan tus mensajes de correo electrónico, ellos pueden escanear toda la información legible que sale e ingresa a tu computadora. En otras palabras, este truco no funcionaría al menos que cada uno se conecte de manera segura a esa cuenta compartida con interfaz web. Y si lo hacen entonces no hace daño a nadie crear cuentas separadas o seguir adelante y pulsar el botón de 'enviar'.

Hace tiempo que es posible asegurar tu conexión de Internet entre tu computadora y los sitios web que visitas. A menudo encuentras este nivel de seguridad cuando ingresas contraseñas o información de tarjeta de crédito en sitios web. La tecnología que hace que ello sea posible se llama *cifrado* [131] de *Capa de Conexión Segura (Secure Sockets Layer (SSL))* [132]. Puedes decir si estas o no utilizando SSL mirando con atención la barra de direcciones de tu navegador web.

Todas las direcciones web normalmente empiezan con las letras **HTTP**, como se muestra en el ejemplo siguiente:

Cuando visitas un sito web seguro, su dirección empieza con **HTTPS**.

La '**S**' adicional al final significa que tu computadora ha establecido una conexión segura al sitio web. También puedes notar un símbolo de 'candado', ya sea en la barra de direcciones o en la barra de estado en la parte baja de tu ventana del navegador. Estas son pistas que te permiten saber que cualquiera que esté vigilando tu conexión a Internet no será ya capaz de espiar tu comunicación con dicho sitio web en particular.

Además de proteger contraseñas y transacciones financieras, este tipo de *cifrado* [131] es perfecto para asegurar tu correo con interfaz web. Sin embargo, muchos proveedores de correos con interfaz web no ofrecen acceso seguro, y otros requieren que lo habilites explícitamente, ya sea fijando una preferencia o ingresando manualmente el término **HTTPS**. Siempre debes asegurarte que tu conexión sea segura antes de tener acceso, leer tu correo electrónico o enviar un mensaje.

Debes prestar mucha atención si tu navegador de pronto empieza a quejarse sobre unos *certificados de seguridad* [133] inválidos cuando intentas acceder a una cuenta segura con interfaz web. Esto podría significar que alguien esta

interfiriendo en la comunicación entre tu computadora y el servidor con el fin de interceptar tus mensajes. Finalmente, si confías en tu correo con interfaz web para intercambiar información sensible, es importante que tu navegador sea lo más confiable posible. Considera el instalar Mozilla *Firefox* [134] y sus complementos vinculados a la seguridad.

Parte Práctica: Empieza con la Guía del Firefox [113]

Pablo: Una de las personas que va a trabajar con nosotros en este informe tiende a utilizar su cuenta de correo con interfaz web de Yahoo cuando no está en la oficina. Y si no recuerdo mal alguien más utiliza Hotmail. Si les envío un mensaje a estas personas, ¿Puede otra persona leerlos?

Claudia: Probablemente. Yahoo, Hotmail y otros muchos proveedores de correo con interfaz web tienen sitios web inseguros que no protegen la privacidad de los mensajes de sus usuarios. Vamos a tener que cambiar los hábitos de ciertas personas si deseamos ser capaces de tratar estos testimonios de forma segura.

Cambiarse a una cuenta de correo electrónico más segura

Pocos proveedores de correo con interfaz web ofrecen el acceso *Capa de Conexión Segura (SSL)* [132] a tu correo electrónico. Por ejemplo, Yahoo y Hotmail, proporcionan una conexión segura cuando inicias sesión, para proteger tu contraseña, pero tus mensajes en sí se envían y reciben de manera insegura. Además, Yahoo, Hotmail y otros proveedores de correo con interfaz web incluyen la *dirección IP* [135] de la computadora que estas utilizando en todos los mensajes que envías.

Las cuentas de Gmail, por otro lado, utilizan una conexión segura desde el inicio de sesión y todo el tiempo hasta que hayas cerrado la sesión. Puedes comprobarlo todo el tiempo viendo y observando el URL que inicia con 'https', en la que la 's' denota una conexión segura. A diferencia de Yahoo y Hotmail, el Gmail no revela tu dirección IP a tus destinatarios de correo. Sin embargo no es recomendable que confíes completamente en Google para la confidencialidad de tus comunicaciones electrónicas sensibles. Google escanea y guarda el contenido de los mensajes de sus usuarios para una gran variedad de propósitos y, en el pasado, ha sido condesciente con demandas de los gobiernos que restringen la libertad digital. Dirígete a la sección de **Lecturas Adicionales** [136] para obtener mayor información sobre la política de privacidad de Google.

Si es posible, debes crearte una nueva cuenta de correo electrónico en *Riseup* [137] visitando https://mail.riseup.net [138]. Riseup ofrece correo electrónico gratuito a los activistas alrededor del mundo y presta mucha atención a la protección de la información almacenada en sus servidores. Ellos por mucho tiempo han sido una fuente confiable para aquellos con necesidad de soluciones seguras de correo electrónico. Y, a diferencia de Google, tiene políticas muy estrictas relativas a la privacidad de sus usuarios e intereses no comerciales que en algún momento pudieran entrar en conflicto con sus políticas. Sin embargo, con el fin de crear una nueva cuenta de Riseup, necesitaras dos 'códigos de invitación.' Estos pueden ser entregados por cualquiera que ya tenga una cuenta de Riseup. Si tienes una copia física de este folleto, debes haber recibido tus 'códigos de invitación' junto con el mismo. Si no es así, necesitaras ubicar dos usuarios de Riseup y solicitarles que cada uno de ellos te envíe un código.

Parte Práctica: Empieza con la Guía del Riseup [139]

Tanto el Gmail como *Riseup* [137] son más que solo proveedores de correo con interfaz web. Estos pueden también utilizarse con un cliente de correo electrónico, tal como el Mozilla *Thunderbird* [140], que admite las técnicas descritas en **Seguridad avanzada de correo electrónico** [125]. El garantizar que tu cliente de correo electrónico tenga una conexión *cifrada* [131] con tu proveedor es tan importante como el acceder a tu correo con interfaz web a través de una dirección **HTTPS** Si utilizas un cliente de correo electrónico, dirígete a la **Guía del Thunderbird** [141] para detalles adicionales. Sin embargo, por lo menos, debes estar seguro de habilitar el cifrado *SSL* [132] o **TLS** tanto para los servidores de correo de salida como de entrada.

Pablo: Entonces, ¿debo cambiarme a utilizar el Riseup o puedo seguir utilizando Gmail, y simplemente cambiarme a una dirección 'https'?

Claudia: Esa es tu decisión, pero hay algunas cosas que debes considerar definitivamente cuando elijas un proveedor de correo electrónico. Primero, ¿te ofrecen una conexión segura a tu cuenta? Gmail lo hace, entonces ahí estás bien. Segundo, ¿confías en que los administradores mantengan privado tu correo electrónico y que no lo lean o compartan con otros? Esa depende de ti. Y, finalmente, debes pensar si es o no aceptable para ti que se te identifique con ese

proveedor. En otras palabras, te pondrá en problemas el utilizar una dirección de correo electrónico que termine con 'riseup.net', el cual se conoce que es popular entre activistas, o necesitas una dirección más común como 'gmail.com'?

Sin importar que herramientas seguras de correo electrónico decidas utilizar, considera que cada mensaje tiene un remitente y uno o más destinatarios. Tú mismo eres sólo una parte de todo, incluso si accedes a tu cuenta de correo electrónico de manera segura, considera que precauciones toman o no tus contactos cuando envían, leen y responden a los mensajes, trata también de conocer dónde se hallan los proveedores de correo electrónico de tus contactos.

Naturalmente, algunos países son más agresivos que otros cuando se trata de vigilancia de correos electrónicos. Para garantizar la comunicación privada, tú y tus contactos deben utilizar servicios de correo electrónico seguros alojados en países relativamente seguros. Y - si quieres estar seguro que tus mensajes no son interceptados entre tu servidor de correo electrónico y el correspondiente de tu contacto - todos deben elegir el utilizar cuentas del mismo proveedor, utilizar el *Riseup* [137] es una buena idea.

Consejos adicionales para mejorar la seguridad de tu correo electrónico

- Siempre se cauto cuando abras archivos adjuntos de un correo electrónico que no estés esperando, que provenga de alguien que no conoces o que contengan términos sospechosos en la línea de asunto. Cuando abras correos electrónicos como estos, debes asegurarte que tu antivirus esté actualizado y prestar mucha atención a cualquier advertencia que se muestre por parte de tu navegador o tu programa de correo electrónico.
- El utilizar software anónimo como el *Tor* [142], el cual se describe en el capítulo **8. Mantenerse en el anonimato y evadir la censura en Internet** [143], puede ayudarte a esconder el servicio de correo electrónico que elegiste de cualquiera que pudiera estar vigilando tu conexión de Internet. Y, dependiendo de la amplitud del filtrado de Internet en tu país, podrías necesitar utilizar Tor, o una de las herramientas de *evasión* [144] descritas en dicho capitulo, sólo para acceder a un proveedor seguro de correo electrónico tal como el *Riseup* [137] o Gmail.
- Cuando crees una cuenta que pretendes utilizar mientras te mantienes anónimo antes tus propios destinatarios de correo electrónico, o de foros públicos en los cuales colocas mensajes por correo electrónico, debes ser lo suficientemente cuidadoso para no registrar un nombre de usuario o 'Nombre Completo' que este relacionado a tu vida personal o profesional. En dichos casos, también es importante que evites utilizar Hotmail, Yahoo, o cualquier otro proveedor de correo con interfaz web que incluya tu *dirección IP* [135] en los mensajes que envías.
- Dependiendo de quien tenga acceso físico a tu computadora, el eliminar los rastros vinculados a tu correo electrónico de tus archivos temporales puedes ser tan importante como proteger tus mensajes mientras viajan por la Internet. Dirígete al capítulo **6. Destruir información sensible** [145] y a la **Guía del CCleaner** [146] para obtener detalles.

Consejos para responder ante una sospecha de vigilancia de correo electrónico

Si sospechas que alguien ya está vigilando tu correo electrónico, puedes querer crear una nueva cuenta y conservar la antigua como un señuelo. Sin embargo, recuerda que cualquier cuenta con la cual hayas intercambiado correo electrónico en el pasado podría estar también ahora bajo vigilancia. Como resultado de ello, debes tener algunas precauciones adicionales:

- Tanto tú como tus contactos recientes de correo electrónico deben crear nuevas cuentas y conectarse a ellas sólo desde lugares, como un café Internet, que nunca antes hayan utilizado. Te recomendamos esta estrategia con el fin de evitar conexiones desde la computadora que normalmente usas, la cual puede estar vigilada, y facilitarles a quienes te vigilan la ubicación de tu nueva cuenta. Como alternativa—si vas a iniciar sesión para tu nueva cuenta desde tu ubicación normal—puedes utilizar una de las herramientas descritas en el capítulo **8. Mantenerse en el anonimato y evadir la censura en Internet** [147], para ocultar estas conexiones.
- Intercambia información sobre esta nueva dirección de correo electrónico solo a través de canales seguros, tales como reuniones cara a cara, mensajes instantáneos seguros o cifrados, conversaciones de *Voz sobre Protocolo de Internet (VoIP)* [119].
- Mantén casi sin cambios el tráfico en tu vieja cuenta, al menos por un tiempo. Debes aparentar ante el espía que todavía estas utilizando la cuenta para información sensible. Probablemente, desees evitar el revelar información vital, pero debes intentar no hacer obvio que lo estás haciendo. Como puedes imaginar, esto puede ser algo exigente.
- Dificulta el conectar tu identidad real con tu nueva cuenta. No envíes correos electrónicos entre tu nueva cuenta y las antiguas (o las de cualquier contacto del que sospeches que también pueda estar vigilado).
- Mantente atento a lo que escribes cuando utilices tu nueva cuenta. Es mejor que evites utilizar nombres reales y direcciones o frases como 'derechos humanos' o 'tortura.' Desarrolla un sistema de código informal con tus contactos de correo electrónico y cámbialo periódicamente.
- Recuerda. La seguridad del correo electrónico no trata solamente de tener fuertes defensas técnicas. Es también

prestar atención a como tú y tus contactos de correo electrónico se comunican y mantienen disciplinados con relación a sus hábitos no técnicos de seguridad.

Asegurar otras herramientas de comunicación por Internet

De manera similar que en el caso del correo electrónico, el software de mensajería instantánea y de *Voz sobre Protocolo de Internet (VoIP)* [148] pueden o no ser seguros, dependiendo de las herramientas que escojas y de cómo las uses.

Asegurar tu software de mensajería instantánea

La mensajería instantánea, también llamada 'chat,' normalmente no es segura, y puede ser tan vulnerable a la vigilancia como lo es el correo electrónico. Por suerte, existen programas que pueden ayudarte a asegurar la privacidad de tus sesiones de conversación o chat. Sin embargo - del mismo modo que con el correo electrónico - un canal de comunicación seguro requiere que tanto tú como tus contactos de mensajería instantánea utilicen el mismo software y tomen las mismas precauciones de seguridad.

Existe un programa de chat llamado *Pidgin* [149] que admite muchos de los protocolos existentes de mensajería instantánea, lo que significa que puedes utilizarlo fácilmente sin tener que cambiar el nombre de tu cuenta o recrear tu lista de contactos. Con el fin de tener conversaciones privadas **cifradas** a través del Pidgin, necesitarás instalar y activar el complemento *Fuera de Registro (OTR)* [150]. Afortunadamente, este es un proceso muy simple.

Parte Práctica: Empieza con la Guía del Pidgin [151]

Pablo: Si el correo con interfaz de Yahoo es inseguro, eso significa que el ¿Yahoo Chat es inseguro, también?

Claudia: Lo que tienes que recordar es que, si queremos utilizar mensajería instantánea para ocuparnos de este informe, necesitamos asegurarnos que todas las personas involucradas tengan instalados el Pidgin y el complemento Fuera de Registro (OTR). Si es así, podemos utilizar el Yahoo Chat o cualquier otro servicio de conversación (Chat).

Asegurar tu software de Voz sobre Protocolo de Internet (VoIP)

Las llamadas utilizando *Voz sobre Protocolo de Internet (VoIP)* *[148]* hacia otros usuarios de Voz sobre Protocolo de Internet (VoIP) son generalmente gratuitas. Algunos programas te permiten también hacer llamadas baratas a teléfonos normales, incluyendo números internacionales. No es necesario decir que estas características pueden ser extremadamente útiles. Algunos de los programas más populares de Voz sobre Protocolo de Internet (VoIP) incluyen al *Skype* [152], Jitsi [153] [1], Google Talk [154] [2], Yahoo! Voice [155] [3] y el MSN Messenger [156] [4].

Normalmente, la comunicación por voz en Internet no es más segura que el correo electrónico no protegido y la mensajería instantánea. Cuando utilices conversaciones por voz para el intercambio de información sensible es importante escoger una herramienta que cifre la llamada durante todo el proceso desde tu computadora hasta la computadora del destinatario. También es mejor utilizar software libre y de código abierto, preferiblemente aquellos que han sido revisados, probados y recomendados por una comunidad confiable. Tomando en cuenta los criterios expuestos anteriormente, recomendamos que pruebes Jitsi como tu elección para VoIP.

Nota sobre la seguridad de Skype

El *Skype* [152] es una herramienta común de mensajería instantánea y de VoIP que también soporta llamadas a líneas fijas y teléfonos móviles. A pesar de su popularidad, varios temas hacen de esta aplicación un elección insegura. Algunos de estos temas se describen a continuación.

Según indica Skype, encriptan tanto los mensajes comos las llamadas de voz, esto sólo sucedería cuando ambos lados de la comunicación se encuentren utilizando el programa Skype. Skype no cifra las llamadas a teléfonos o textos

enviados por mensajes SMS.

Si ambos lados de la comunicación se encuentran utilizando el programa (genuino) Skype, su cifrado podrá hacer un poco más segura la llamada que aquellas realizadas de forma común por teléfono. Pero debido a que Skype es una programa de código cerrado, es imposible realizar una auditoría independiente y una evaluación de sus afirmaciones sobre cifrado, así mismo es imposible verificar que tan bien protege Skype a sus usuarios/as y su información y comunicación. El capitulo **1. Proteger tu computadora de software malicioso (malware) y piratas informáticos (hackers)** [128] se ocupa de las virtudes del *Software Libre y de Código Abierto (FOSS)* [13] en su sección **mantener actualizado tu software**.

Como mencionamos anteriormente, no podemos recomendar Skype como herramienta segura de comunicación, es importante tomar algunas precauciones si uno/a decide utilizarlo para comunicar información sensible:

Descargue e instale Skype sólo de su sitio oficial www.skype.com [157] para evitar un programa skype infectado con spyware. Siempre es importante que revises dos veces el URL para asegurarte de que estas conectado al sitio oficial. En algunos países el sitio de Skype está bloqueado y/o algunos sitios falsos anunciando que son el sitio oficial de Skype están funcionando. En estos casos, la versión disponible de Skype seguramente está infectado con malware diseñado para espiar cualqueir comunicación. Utiliza herramientas de evasión como se describe en el Capítulo 8 para conectarse al sitio de Skype y descargar una versión genuina del programa Skype y cuando quieras actualizar la última versión del programa.

Es importante que cambies tu contraseña de Skype regularmente. Skype permite múltiples accesos a sesiones desde diferentes ubicaciones y no te informa de estas múltiples sesiones simultáneas. Esto es un gran riesgo si tu contraseña se encuentra comprometida, porque cualqueira con esa contraseña puede abrir su sesión. Todas las sesiones abiertas reciben todas las comunicaciones de texto y tienen acceso al historial de llamadas. Cambiar la contraseña es la única forma de deshabilitar las sesiones 'ilegales' (obligando a un reinicio de sesión).

También es recomendable activar las configuraciones de privacidad del Skype para que no guarde el historial de los chat.

También es recomendable deshabilitar la configuración del Skype que permite aceptar automáticamente los archivos enviados, ya que esto ha sido utilizado para introducir malware/spyware en las computadoras.

Siempre verifica de forma independiente la identidad de la persona con quien te estás comunicando. Es más sencillo hacerlo cuando realizas chat con voz ya que sabes con quién estás hablando.

Decide si quieres que tu nombre de usuario te identifica o relaciona con tu nombre verdadero o el nombre de tu organización.

Es importante siempre buscar otras alternativas de comunicación. Skype podría no estar disponible en todo momento.

Ten cuidado con lo que dices, desarrolle un sistema de código para conversar sobre temas sensibles sin utilizar una terminología específica.

A pesar de la popularidad de Skype, las preocupaciones anteriormente expuestas cuestionan su uso seguro, por lo tanto recomendamos que inicies el uso de herramientas como Jitsi para VoIP y Pidgin, con el complemento Fuera de Registro (OTR), para mensajería instantánea segura.

Seguridad avanzada de correo electrónico

Las herramientas y conceptos tratados a continuación se recomiendan para usuarios de computadoras experimentados.

Utilizar cifrado de clave (llave) pública en correo electrónico

Es posible alcanzar un gran nivel de privacidad con el correo electrónico, incluso con una cuenta de correo electrónico insegura. Para hacer esto, necesitas aprender sobre [**cifrado**] (/es/glossary#Cifrado) de clave pública. Esta técnica te permite cifrar mensajes individuales, haciéndolos ilegibles a cualquiera que no sea uno de los destinatarios previstos. El aspecto ingenioso del cifrado de clave pública es que no tiene que intercambiar ninguna información secreta con tus contactos sobre cómo vas a cifrar tus mensajes en el futuro.

Pablo: ¿Pero como funciona todo esto?

Claudia: ¡Puras matemáticas! Cifras tus mensajes hacia un contacto de correo electrónico dado, utilizando su 'clave pública' especial la cual puede distribuir libremente. Luego, ella utiliza su 'clave privada,' la cual debe guardar cuidadosamente, con el fin de leer dichos mensajes. A su turno, tu contacto utiliza su clave pública para cifrar mensajes que te escribe. De modo que al final, debes intercambiar claves públicas, pero puedes compartirlas abiertamente, sin tener que preocuparte sobre el hecho de que cualquiera que desee tu clave pública pueda obtenerla.

Esta técnica puede utilizarse con cualquier servicio de correo electrónico, incluso con uno que no cuente con un canal de comunicación seguro, debido a que los mensajes individuales son [**cifrados**] (/es/glossary#Cifrado) antes de que dejen tu computadora.

Recuerda que al utilizar el [**cifrado**] (/es/glossary#Cifrado) puedes atraer la atención hacia ti. El tipo de [**cifrado**]

(/es/glossary#Cifrado)utilizado cuando accedes a un sito web seguro, incluyendo una cuenta de correo con interfaz web, se ve a menudo con menor sospecha que la del tipo de [**cifrado**] (/es/glossary#Cifrado) de clave pública del que nos ocupamos aquí. En algunas circunstancias, si un correo electrónico que contenga esta suerte de datos [**cifrados**] (/es/glossary#Cifrado) es interceptado o publicado en un foro público, podría incriminar a la persona que lo envió, sin considerar el contenido del mensaje. Tú a veces tendrías que escoger entre la privacidad de tu mensaje y la necesidad de mantenerte sin llamar la atención.

Cifrar y autenticar mensajes individuales

El [**cifrado**] (/es/glossary#Cifrado) de clave pública puede parecer complicado al inicio, pero es muy directo una vez que has entendido los fundamentos, y las herramientas no son difíciles de utilizar. Simple, de fácil uso para el usuario y portátil, así es el programa **gpg4usb** el cuál puede cifrar textos y archivos para mensajes de correo electrónico incluso cuando no estás conectado a la Internet.

Parte Práctica: Empieza con *gpg4usb Portátil - guía del programa de cifrado de texto y archivos para mensajes de correo electrónico* [158]

El programa de correo electrónico de **Mozilla Thunderbird** [141] puede ser utilizado con un complemento llamado **Enigmail** [159] para cifrar y descifrar muy fácilmente mensajes de correo electrónico.

Parte Práctica: Empieza con ** ***Thunderbird cliente de correo seguro* [141]

VaultletSuite 2 Go [160], oftware gratuito de cifrado de correos electrónicos, es incluso más fácil de utilizar que el Thunderbird si optas por confiar en la compañía que lo provee y permitirle a esta realizar parte del trabajo por ti.

Parte Práctica: Empieza con ** ***VaultletSuite 2Go - cliente de correo seguro* [161]

La autenticidad de tu correo electrónico es otro aspecto importante de la seguridad en las comunicaciones. Cualquiera con acceso a la Internet y las herramientas correctas puede suplantarte enviando mensajes desde un correo electrónico falso que sea idéntico al tuyo. El peligro aquí es más aparente cuando se considera desde la perspectiva del destinatario. Imagina, por ejemplo, la amenaza planteada por un correo electrónico que aparenta ser de un contacto confiable pero que es en realidad de alguien cuyo objetivo es el de perturbar tus actividades o conocer información sensible sobre tu organización.

Debido a que no podemos ver o escuchar a nuestros corresponsales a través del correo electrónico, normalmente confiamos en la dirección del remitente para verificar su identidad, que es la razón por la cual somos fácilmente engañados por correos electrónicos falsos. Las **Firmas digitales** [162] - las cuales también se sostienen en el **cifrado** [131] de clave pública - proporcionan un medio más seguro de probar la identidad de uno cuando se envía un mensaje. La guía del ***gpg4usb Portátil*** [158] o la sección ***Utilizar Enigmail con GnuPG en Thunderbird*** [163] de la ***Guía del Thunderbird*** [141] explica en detalle cómo se hace esto.

Pablo: Tengo un colega que una vez recibió un correo electrónico de parte mía que nunca envié. Decidimos, al final, que simplemente era correo comercial no deseado (spam), pero ahora me imagino cuanto daño podría haberse hecho si un correo electrónico falso apareciera en el buzón de la persona equivocada en el momento inapropiado. Escuche que se puede impedir esta clase de evento con firmas digitales ¿pero que son ellas?

Claudia: Una firma digital es como un sello lacrado sobre la solapa de un sobre con tu carta incluida. Excepto que no puede falsificarse. Esto prueba que eres el verdadero remitente del mensaje y que este no ha sido falsificado en el camino.

Lecturas Adicionales

- Para aprender más sobre simular una identidad de correo electrónico, dirígete a la sección de Simulación (Spoofing) [164] del libro Seguridad Digital y Privacidad para Defensores de los Derechos Humanos [30] [5].
- Además de las Guías Prácticas del **Riseup** [165] y de **Thunderbird** [90], existen varios sitios web que explican como utilizar tu programa de correo electrónico con varios proveedores populares de correo electrónico al tiempo de dejar una copia de tus mensajes en el servidor de correo:
  - El sitio web de Riseup [166] [8]
  - Instrucciones para utilizar Gmail [167] [9]
  - Instrucciones para Importar tus contactos de Gmail al Mozilla Thunderbird [168] [10]
  - Para detalles de cómo utilizar otros servicios de correo electrónico de esta manera, busca en la sección de ayuda del sito web del proveedor palabras como 'POP', 'IMAP' y 'SMTP'
- Existe un bien conocido ataque a la seguridad del cifrado de Capa de Conexión Segura (SSL) llamado el ataque del intermediario (Man in the Middle attack) [169] [5].
- La Política de Privacidad de Gmail [170] [6], la cual debes aceptar cuando creas una cuenta de Gmail, explica que, "Google almacena, procesa y mantiene los mensajes, lista de contactos y otros datos relacionado con la cuenta del usuario a fin de suministrarle el servicio." De hecho, todos los proveedores de correo electrónico escanean tus mensajes, hasta cierto punto, de modo que puedan ofrecer servicios contra el correo comercial no solicitado (spam) y otras opciones similares. Sin embargo, el Gmail va un poco más allá para proporcionar 'publicidad dirigida' basada en el contenido real de tu correo electrónico. Esto podría ser peligroso si la información almacenada por Google fuera intencional o accidentalmente expuesta.
- Una serie de entrevistas en el 2008 que se enfocaron en las políticas de privacidad y cifrado [171] [7] de los

principales servicios de mensajería instantánea.

Referencias

[1] www.gizmo5.com/pc [172]
[2] www.google.com/talk [154]
[3] www.voice.yahoo.com [155]
[4] www.download.live.com/?sku=messenger [156]
[5] www.frontlinedefenders.org/manual/en/esecman [38]
[6] https://mail.google.com/mail/help/intl/en/privacy.html [173]
[7] www.news.cnet.com/8301-13578_3-9962106-38.html [174]
[8] http://help.riseup.net/mail/mail-clients [175]
[9] https://mail.google.com/support/bin/topic.py?topic=12805 [176]
[10] www.email.about.com/od/mozillathunderbirdtips/qt/et_gmail_addr.htm [177]

8. Mantenerse en el anonimato y evadir la censura en Internet

Muchos países alrededor del mundo han instalado software que evita que los usuarios dentro de ese país puedan acceder a ciertos sitios web y servicios de Internet. Las compañías, colegios y bibliotecas públicas a menudo utilizan un software similar para proteger a sus empleados, estudiantes y clientes de material que consideran molesto o dañino. Este tipo de tecnología de filtrado viene en diferentes formas. Algunos filtros bloquean sitios de acuerdo a su *dirección IP* [178], mientras otros ponen en su lista negra ciertos *nombres de dominio* [179] o buscan a través de todas las comunicaciones no cifradas en Internet palabras claves específicas.

Sin importar que métodos de filtrado se hallen presentes, casi siempre es posible evadirlos confiando en computadoras intermediarias, fuera del país, para acceder a servicios bloqueados para ti. Este proceso a menudo se llama *evasión* [180] de la censura, o simplemente evasión, y las computadoras intermedias se llaman *proxies* [181]. También existen proxies de diferentes formas. Este capitulo incluye un breve tratamiento de redes de anonimato multiproxy seguido de una descripción más al detalle de proxies de evasión básica y de cual es su forma de funcionamiento.

Ambos métodos son maneras efectivas de evadir los filtros de Internet, aunque el primero es más apropiado si estas dispuesto a sacrificar velocidad con el fin de mantener tus actividades en Internet lo más anónimas posibles. Si conoces y confías en la persona o en la organización que opera tu *proxy* [181], o si el desempeño es más importante para ti que el anonimato, entonces un proxy de *evasión* [180] básica te será más útil.

Contexto

Mansour y Magda son hermanos, en un país de habla árabe, que mantienen una bitácora (blog) en la cual anónimamente hacen público los abusos de derechos humanos y hacen campaña por un cambio político. Las autoridades en su país no han sido capaces de cerrar su sito web, debido a que está alojado en otro país, pero a menudo han intentado conocer la identidad de los administradores de la bitácora (blog) a través de otros activistas. A Mansour y Magda les preocupa que las autoridades sean capaces de vigilar sus actualizaciones y saber quienes son. Además, desean prepararse para cuando finalmente el gobierno filtre su sitio web, para no sólo continuar actualizándolo, sino también que puedan proporcionar un buen consejo de evasión para sus lectores dentro de su propio país, quienes de otro modo perderían acceso a la bitácora (blog).

¿Qué puedes aprender de esta capítulo?

- Acceder a un sitio web que esté bloqueado dentro de tu país
- Evitar que los sitios web que visitas sepan tu ubicación
- Garantizar que ni tu *Proveedor de Servicios de Internet (ISP* [182]*)* *[182]* ni una organización de vigilancia en tu país puedan determinar que sitios web o servicios de Internet visitas

Comprender la censura en Internet

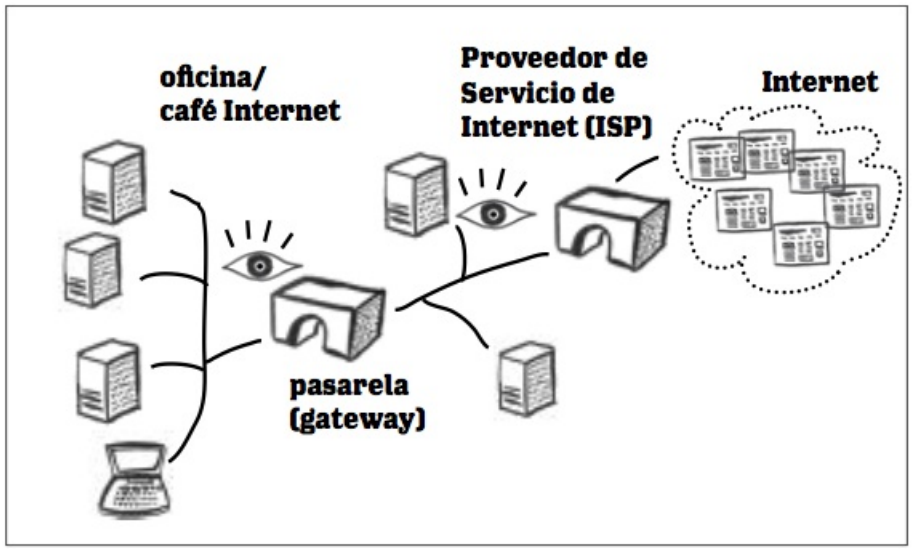
Las investigaciones llevadas a cabo por organizaciones como OpenNet Initiative (ONI) [183] [1] y Reporteros Sin Fronteras (RSF) [184] [2] indican que muchos países filtran una amplia variedad de contenido social, político y de 'seguridad nacional',

aunque raramente publican listas precisas de lo que ha sido bloqueado. Naturalmente, aquellos que desean controlar el acceso de sus ciudadanos a la Internet también hacen un esfuerzo especial para bloquear *proxies* [181] y sitios web conocidos que ofrecen herramientas e instrucciones para ayudar a las personas a evadir estos filtros.

A pesar de la garantía de libre acceso a la información consagrada en el Artículo 19 de la Declaración Universal de los Derechos Humanos, el número de países involucrados en la censura de Internet se ha incrementado espectacularmente en los últimos años. Sin embargo, a medida que la práctica de filtrado de Internet se disemina en el mundo, de igual manera lo hace el acceso a las herramientas de evasión que han sido creadas, utilizadas y publicitadas por activistas, programadores y voluntarios.

Antes de explorar las distintas maneras de evadir la censura en Internet, primero debes desarrollar un entendimiento básico de cómo funcionan estos filtros. Para hacerlo, es muy útil considerar un modelo altamente simplificado de tu conexión a Internet.

Tu conexión a Internet



El primer paso de tu conexión a la Internet se hace típicamente a través del *Proveedor de Servicio de Internet (ISP)* [182] en casa, oficina, colegio, biblioteca o café Internet. El Proveedor de Servicio de Internet (ISP) le asigna a tu computadora una *dirección IP* [178], la cual puede ser utilizada por varios servicios de Internet para identificarte y enviarte información, tales como los correos electrónicos y páginas web que solicites. Cualquiera que conozca tu dirección IP puede saber más o menos en que ciudad te hallas. Sin embargo, algunas organizaciones bien conectadas en tu país, pueden utilizar esta información para determinar tu ubicación precisa.

- **Tu Proveedor de Servicio de Internet (ISP)** sabrá en que edificio estás o que línea telefónica estás utilizando si accedes a Internet a través de un módem.
- **Tu café Internet, biblioteca o negocio** sabrá que computadora estuviste utilizando en un momento determinado, así como a que puerto o a que punto de acceso inalámbrico estuviste conectado.
- **Las agencias gubernamentales** pueden conocer todos estos detalles, como resultado de su influencia sobre las organizaciones arriba mencionadas.

En este punto, tu [185]*Proveedor de Servicio de Internet (ISP)* [182] descansa en la infraestructura de la red en tu país para conectar a sus usuarios, incluyéndote, con el resto del mundo. En el otro extremo de tu conexión, el sitio web o el servicio de Internet al cual estás accediendo pasa a través de un proceso similar, habiendo recibido su propia dirección IP de su Proveedor de Servicio de Internet (ISP) en su propio país. Incluso sin todos los detalles técnicos, un modelo básico como este puede ser útil cuando piensas en las varias herramientas que te permiten rodear los filtros y mantenerte anónimo en la Internet.

Cómo son bloqueados los sitios web

Esencialmente, cuando vas a visualizar una página web, le estás mostrando la *dirección IP* [178] del sitio a tu *Proveedor de Servicio de Internet (ISP)* [182] y solicitándole conectarte con el Proveedor de Servicio de Internet (ISP) del servidor web. Y - si tienes una conexión de Internet no filtrada - hará justamente eso. Sin embargo, si te encuentras en un país que censura la Internet, este consultará primero la *lista negra* [186] de sitios web prohibidos y luego decidirá si accede o no a tu solicitud.

En algunos casos, puede haber una organización central que maneja el filtrado en lugar de los mismos [185]*Proveedor de Servicio de Internet (ISP)* [182]. A menudo, una *lista negra* [187] contendrá *nombres de dominio* [179], tales como www.blogger.com [188], en vez de *direcciones IP* [178]. Y, en algunos países, el software de filtrado controla tu conexión, en vez de intentar bloquear direcciones específicas en Internet. Este tipo de software escanea las solicitudes que hiciste y las páginas que regresan a ti, buscando palabras claves sensibles para luego decidir si te permite o no ver los resultados.

Y, para empeorar las cosas, cuando una página web es bloqueada no podrías ni siquiera saberlo. Aunque algunos filtros proporcionan una 'página de bloqueo' que explica porque una página en particular ha sido censurada, otras muestran mensajes de error desorientadores. Estos mensajes pueden implicar que la página no puede ser encontrada, por ejemplo, o que la dirección fue mal ingresada.

En general, lo más fácil es adoptar la perspectiva correspondiente al peor caso hacia la censura de Internet, en vez de intentar investigar todas las fortalezas y debilidades de las tecnologías de filtrado utilizadas en tu país. En otras palabras, puedes asumir que:

- Tu tráfico en Internet está controlado por palabras claves.
- El filtrado está implementado directamente al nivel del *Proveedor de Servicio de Internet (ISP)* [182].
- Los sitios bloqueados son considerados en *listas negras* [186] tanto por las *direcciones IP* [178] como por *nombres de dominio* [179].
- Se te pueden dar razones oscuras o desorientadoras para explicar porque un sitio bloqueado no se descarga.

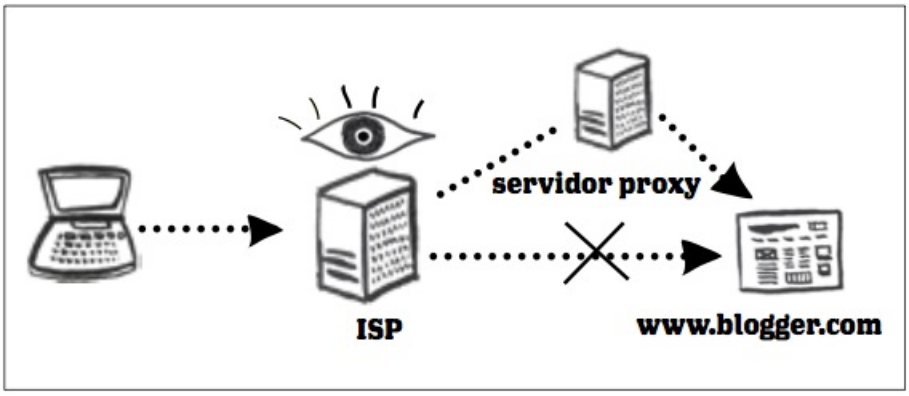
Debido a que las herramientas de evasión más efectivas pueden ser utilizadas sin importar que métodos de filtrado están en funcionamiento, generalmente no hace daño hacer esta asunción pesimista.

Mansour: Entonces, si un día me encuentro con que no puedo acceder a la bitácora (blog), pero un amigo en otro país puede verlo sin problemas, ¿eso significa que el gobierno lo ha bloqueado?

Magda: No necesariamente. Podría ser algún problema que sólo afecta a las personas que están tratando de acceder al sitio web desde aquí. O, podría ser algún problema con tu computadora que sólo se muestra con ciertos tipos de páginas web. Sin embargo estás en la ruta correcta. Podrías también intentar visitarla mientras utilizas una herramienta de evasión. Después de todo, la mayoría de estas herramientas descansan en servidores proxy externos, cuyo funcionamiento se parece al hecho de pedirle a un amigo en otro país que pruebe un sitio web para ti, excepto que puedes hacerlo por ti mismo

Entender la evasión de la censura

Si no puedes acceder directamente a un sitio web debido a que está bloqueado por uno de los métodos tratados anteriormente, necesitas encontrar una forma de rodear la obstrucción. Un servidor *proxy* [181] seguro, localizado en un país que no filtra la Internet puede proporcionar esta clase de desvío buscando las páginas web que solicitas y enviándotelas. Desde la perspectiva de tu *Proveedor de Servicio de Internet (ISP)* [182] aparecerás simplemente comunicándote de manera segura con una computadora desconocida (el servidor proxy) en algún lugar de la Internet.



Obviamente, la agencia gubernamental a cargo de la censura de Internet en tu país—o la compañía que proporciona actualizaciones para su software de filtrado—podría finalmente saber que esta 'computadora desconocida' es realmente un *proxy* [181] de evasión. Si esto ocurre, su *dirección IP* [178] puede ser añadida a la *lista negra* [186], y no funcionará más. Sin embargo, normalmente toma algún tiempo el bloqueado de los proxies, y aquellos quienes crean y actualizan las herramientas de evasión son concientes de esta amenaza. Ellos responden utilizando uno o los dos métodos mostrados a continuación:

- Los **Proxies escondidos** son más difíciles de identificar. Esta es una de las razones por la que es importante utilizar *proxies* [181] seguros, los cuales son menos obvios. Sin embargo, el *cifrado* [48] es sólo parte de la solución. Los operadores de un proxy también deben ser cuidadosos cuando dan su ubicación a nuevos usuarios si desean que este se mantenga escondido.

- Los **Proxies desechables** pueden ser reemplazados muy rápidamente después de ser bloqueados. El proceso de informar a los usuarios como hallar los *proxies* [181] de reemplazo puede no ser particularmente seguro. En vez de ello, las herramientas de evasión de este tipo a menudo simplemente tratan de distribuir nuevos proxies más rápido que su proceso de bloqueo.

Al final, mientras sea posible tener a la mano un *proxy* [181] confiable para que te traiga los servicios que solicitas, todo lo que debes hacer es enviar tu solicitud y ver que regrese utilizando la aplicación apropiada de Internet. Normalmente, los detalles de este proceso son manejados automáticamente por el software de evasión que instalaste en tu computadora, al modificar las opciones de tu navegador o dirigiendolo a una página proxy basada en la web. La red anónima *Tor* [189], descrita en las sección siguiente, utiliza el primer método. A continuación viene el tópico de herramientas de evasión proxy básicas, únicas, cada una de las cuales funciona de manera ligeramente diferente.

Redes anónimas y servidores proxy básicos

Redes anónimas

Las redes anónimas normalmente 'hacen rebotar' tu tráfico de Internet entre varios *proxies* [181] seguros con el fin de disfrazar de donde vienes y a que estas tratando de acceder. Esto puede reducir significativamente la velocidad a la cual eres capaz de descargar las páginas web y otros servicios de Internet. Sin embargo, en el caso de *Tor* [189], este también te proporciona un medio confiable, seguro y público de evasión que te ahorra el preocuparte si confías o no en las personas que operan tus proxies y los sitios web que visitas. Como siempre, debes garantizar que tienes una conexión cifrada, utilizando *HTTPS* [190], para un sitio web seguro antes de intercambiar información sensible, tal como contraseñas y correos electrónicos, a través de un navegador.

Tienes que instalar software para utilizar el *Tor* [189], pero el resultado es una herramienta que te proporciona anonimato así como evasión. Cada vez que te conectas a la red del Tor, seleccionas una ruta aleatoria a través de tres proxies seguros del Tor. Esto garantiza que ni tu *Proveedor de Servicio de Internet (ISP)* [182] ni los mismos proxies conozcan tanto la *dirección IP* [178] de tu computadora y al mismo tiempo la ubicación de los servicios de Internet que solicitas. Puedes aprender más sobre esta herramienta en la Guía del Tor.

Parte Práctica: Empieza con la Guía del Tor [191]

Una de las fortalezas del *Tor* [189] es que no solo trabaja con navegador sino que puede ser utilizado con varios tipos de software de Internet. Los programas de correo electrónico, entre ellos el Mozilla *Thunderbird* [26], y los programas de mensajería instantánea, incluyendo al *Pidgin* [122], pueden ser operados a través del Tor, ya sea para acceder a servicios filtrados o para esconder el uso que le das a dichos servicios.

Proxies básicos de evasión

Existen tres importantes características que debes considerar cuando seleccionas un *proxy* [181] básico de evasión. Primero, ¿es una herramienta basada en la web? o ¿requiere que cambies las opciones o que instales software en tu computadora? Segundo, ¿es seguro? Tercero, ¿es público o privado?

Proxies basados en la web y otros:

Los *proxies* [181] basados en la web son probablemente los más fáciles de usar. Ellos sólo requieren que apuntes tu navegador hacia una página web proxy, ingreses la dirección filtrada que deseas ver y pulses un botón. El proxy entonces mostrará el contenido solicitado dentro de su propia página web. Puedes normalmente seguir los enlaces o ingresar una nueva dirección en el proxy si deseas ver una nueva página. No necesitas instalar ningún software o cambiar alguna opción de navegador, lo cual significa que los proxies basados en la web son:

- Fáciles de usar
- Asequibles desde computadoras públicas, como aquellas en los cafés Internet, las cuales no podrían permitirte instalar programas o cambiar opciones
- Son potencialmente seguros si estás preocupado acerca de ser 'sorprendido' con software de evasión en tu computadora.

Los *proxies* [181] basados en la web también tienden a tener ciertas desventajas. No siempre muestran correctamente las páginas, y muchos proxies basados en la web no lograrán descargar sitios web complejos, entre ellos los que presentan archivos de audio simultáneo y contenido de video. Además, mientras que un proxy se hará mas lento mientras sea utilizado por más usuarios, esto podría ser más problemático con los proxies públicos basados en la web. Y, obviamente, los proxies basados en la web sólo funcionan para páginas web. No puedes, por ejemplo, utilizar un programa de mensajería instantánea o un cliente de correo electrónico para acceder a servicios bloqueados a través de un proxy basado en la web. Finalmente, los proxies seguros basados en la web ofrecen una confidencialidad limitada debido a que ellos mismos deben acceder y modificar la información de retorno hacia ti proveniente de los sitios web que visitas. Si no lo hicieran, serías incapaz de pulsar en un enlace sin dejar atrasado al proxy e intentar hacer una conexión directa hacia la página web objetivo. Esto se trata más adelante en la sección siguiente.

Otros tipos de *proxies* [181] generalmente requieren que instales un programa o configures una dirección externa de un proxy en tu navegador o sistema operativo. En el primer caso, tu programa de evasión normalmente proporcionará alguna forma de activar y desactivar la herramienta, para indicarle a tu navegador si debe o no utilizar el proxy. El software de este tipo a menudo te permite cambiar automáticamente de proxies si uno de ellos es bloqueado, como se trató anteriormente. En el segundo caso, necesitarás saber la dirección correcta del proxy, la cual cambiará si dicho proxy es bloqueado o se vuelve tan lento que se convierta en inútil.

Aunque esto puede ser ligeramente más difícil de utilizar que un *proxy* [181] basado en la web, este método de evasión esta mejor dotado para mostrar páginas complejas de manera correcta y le tomará mucho más tiempo ralentizarse a medida que las personas utilicen un proxy dado. Además, pueden encontrarse proxies para varias aplicaciones diferentes de Internet. Los ejemplos incluyen proxies HTTP para navegadores, SOCKS para programas de correo electrónico y mensajería (chat) y VPN que pueden redireccionar todo tu tráfico de Internet para evitar el filtrado.

Proxies seguros e inseguros:

Un *proxy* [181] seguro, en este capitulo, se refiere a cualquier proxy que permita conexiones *cifradas* *[48]* de sus usuarios. Un proxy inseguro te permitirá evadir muchos tipos de filtro pero fracasará si tu conexión de Internet esta siendo escaneada en busca de palabras claves o de direcciones de páginas web. Es especialmente malo utilizar un proxy inseguro para acceder a sitios web que normalmente están cifrados, tales como aquellos de cuentas de correo electrónico con interfaz web y páginas web bancarias. Al hacerlo, podrías estar exponiendo información sensible que normalmente estaría escondida. Y, como se mencionó anteriormente, los proxies inseguros a menudo son más fáciles de descubrir y bloquear por parte de aquellos que actualizan el software y la políticas de filtrado de Internet. Al final, el hecho de que existan proxies libres, rápidos, seguros significa que existen muy pocas razones para decidirse por uno inseguro.

Tu sabrás si un *proxy* [181] basado en la web es seguro o inseguro si puedes acceder a las mismas páginas web del proxy utilizando direcciones *HTTPS* [190]. Del mismo modo que con los servicios de correo con interfaz web, las conexiones seguras e inseguras pueden ser admitidas, de modo que debes estar seguro de utilizar una dirección segura. A menudo, en dichos casos, deberás aceptar una 'advertencia de certificado de seguridad' de tu navegador con el fin de continuar. Este es el caso para los proxies *Psiphon* [192] y *Peacefire* [193], que se tratan a continuación. Advertencias como estas te indican que alguien, como tu *Proveedor de Servicio de Internet (ISP)* [182] o un *pirata informático (hacker)* [1], podría estar vigilando tu conexión al proxy. A pesar de estas advertencias, es una buena idea utilizar proxies seguros en la medida de lo posible. Sin embargo, cuando confíes en tales proxies para evasión, debes evitar visitar sitios web seguros, ingresar contraseñas o intercambiar información sensible a menos que verifiques la huella digital *Capa de Conexión Segura (SSL)* [194] del proxy. Con el fin de hacer esto, necesitarás una manera de comunicarte con el administrador del proxy.

El Apéndice C de la Guía de Usuario del Psiphon [195] [3] explica los pasos que tanto tú, como el administrador del *proxy* [181] deben dar para verificar la huella digital del proxy.

También debes evitar acceder a información sensible a través de un *proxy* [181] basado en la web a menos que confíes en la persona que lo dirige. Esto se aplica sin importar si ves o no una advertencia de certificado de seguridad cuando visitas el proxy. Incluso se aplica si conoces lo suficiente al operador del proxy para verificar la huella digital del servidor antes de dirigir tu navegador a aceptar la advertencia. Cuando confías en un único proxy para la evasión, su administrador conocerá en todo momento tu *dirección IP* *[178]* y el sitio web al que estás accediendo. Sin embargo, es mucho más importante considerar que si ese proxy está basado en la web, un operador malicioso podría tener acceso a toda la información que pasa entre tu navegador y los sitios web que visitas, incluyendo el contenido de tu correo con interfaz web y tus contraseñas.

Para los *proxies* [181] que no están basados en la web, debes investigar un poco para determinar si admiten conexiones seguras o inseguras. Todas los proxies y las redes anónimas recomendadas en este capitulo son seguros.

Proxies privados y públicos:

Los *proxies* [181] públicos aceptan conexiones de cualquiera, mientras que los privados normalmente requieren un nombre de usuario y una contraseña. Mientras que los proxies públicos tienen la obvia ventaja de estar disponibles libremente, asumiendo que puedan ser hallados, estos tienden a saturarse muy rápidamente. Como resultado de ello, aunque los proxies públicos sean técnicamente tan sofisticados y bien mantenidos como los privados, estos son a menudo relativamente lentos. Finalmente, los proxies privados tienden a ser dirigidos ya sea por lucro o por administradores que crean cuentas para sus usuarios a quienes conocen personal o socialmente. Debido a esto, es generalmente muy fácil determinar que motiva a un operador de un proxy privado. Sin embargo, no debes asumir que los proxies privados son por tanto básicamente más confiables. Después de todo, motivos de lucro han conducido en el pasado a los servicios en línea a exponer a sus usuarios.

Proxies [181] simples, inseguros y públicos pueden a menudo encontrarse ingresando términos como 'proxy público' en un buscador, pero no debes confiar en proxies descubiertos de esta manera. Dada la oportunidad, es mejor utilizar un proxy seguro y privado conducido por personas que conoces y en las que confías, ya sea personalmente o por su reputación, y quienes tienen las habilidades técnicas para mantener su servidor seguro. Ya sea que utilices o no un proxy basado en la web dependerá de tus particulares necesidades y preferencias. En cualquier momento en que utilices un proxy para evasión, es una buena idea utilizar también el navegador *Firefox* [16] e instalar el complemento *NoScript* [17], como se trató en la **Guía del Firefox** [19]. El hacerlo puede ayudarte a protegerte tanto de proxies maliciosos como de sitios web que pueden tratar de descubrir tu verdadera *dirección IP* *[178]*. Finalmente, ten en cuenta que incluso un proxy *cifrado* [48] no tornará un sitio web inseguro en uno seguro. Debes garantizar que tienes una conexión *HTTPS* [190] antes de enviar o

recibir información sensible.

Si eres incapaz de encontrar en tu país una persona, una organización o una compañía cuyo servicio *proxy* [181] consideres confiable, asequible y accesible, debes pensar en utilizar la red anónima del *Tor* [189], de la cual nos ocupamos anteriormente en la parte de **Redes anónimas** [196].

Proxies específicos de evasión

A continuación hay unas cuantas herramientas y *proxies* [181] específicos que pueden ayudarte a evadir el filtrado de Internet. Nuevas herramientas de evasión son producidas regularmente, y las existentes son actualizadas frecuentemente, por tanto para saber más debes visitar el sitio web en línea de la **Caja de Herramientas de Seguridad**, y los sitios mencionados en las sección de **Lecturas Adicionales** [197] que se halla a continuación.

Red Virtual Privada (VPN por sus siglas en inglés) basado en proxies

Los VPN proxy que se describen a continuación hacen que tu conexión completa a internet pasen por el proxie mientras estés conectado/a. Esto puede ser de mucha utilidad si usas proveedores de correo electrónico o mensajería instantánea que se encuentran filtrados en su país.

Riseup VNP. Es para usuarios que tienen cuentas de correo en el servidor de Riseup. El colectivo ofrece la posibilidad de conectarse a un servidor con un VPN proxy gratuito, privado y seguro. Por favor, lea más sobre Riseup VPN y sobre cómo conectarte a él.

Hotspot Shield, es un proxy de evasión público, seguro, VPN y gratuito. Para utilizarlo, necesitas descargar la herramienta [198] [5] e instalarla. La compañía que desarrolla el Hotspot Shield recibe fondos de anunciantes, de modo que veras una 'pancarta publicitaria' en la parte superior de la ventana de tu navegador cada vez que lo uses para visitar sitios web que no proporcionan *cifrado* [48]. A pesar de que es imposible de verificar, esta compañía afirma borrar la *dirección IP* [178] de quienes utilizan la herramienta, en vez de almacenarla o enviarla a sus anunciantes.

Your-Freedom es un *proxy* [181] de evasión privado, seguro y no basado en la web. Esta es una herramienta de *software gratuito (freeware)* [7] que puede utilizarse para acceder a un servicio de evasión sin costo. También puedes pagar un cargo para acceder a un servicio comercial, el cual es más rápido y tiene mucho menos limitaciones. Con el fin de utilizar *Your-Freedom* [199], necesitarás descargar la herramienta [200] [7] y crear una cuenta [201] [8], ambas acciones pueden realizarse en el sitio web de Your-Freedom [202] [9]. De manera similar necesitarás configurar tu navegador para utilizar el proxy OpenVPN cuando te conectes a la Internet. Puedes leer mas en sitio web del Proyecto Sesawe [203] [10].

Freegate es un proxy de evasión público, seguro, VPN y gratuito. Puedes descargar la última versión de Freegate o leer un artículo muy interesante sobre el mismo.

SecurityKISS es un proxy de evasión público, seguro, VPN y gratuito. Para usarlo debes descargar y correr un programa gratuito. No hay necesidad de registrar una cuenta. Los usuarios/as de forma gratuita están restringidos a utilizar un límite diario de 300MB del tráfico de internet por medio del proxy. Para los/as suscriptores/as no existen restricciones y más servidores CPN para usar. Por favor vea la página principal de SecureKISS para aprender más.

Psiphon3 es un proxy de evasión gratuito SSH, VPN público y seguro. Para usarlo necesitas solicitar un enlace del program gratuito que te preparará para usar el proxy. Para solicitarlo envíe un correo electrónico a get@psiphon3.com [204]. Por favor ver la página principal de Psiphon3.

Proxy Web

Psiphon2 es un sistema de servidores proxy web privado y anónimo. Para utilizar psiphon2 [205] [4] necesitas la dirección web (URL) del servidor proxy y una cuenta (nombre de usuario y contraseña). Puedes recibir una invitación para crear una cuenta en el psiphon2 de un usuario que ya tenga una cuenta de este tipo. También puedes utilizar la invitación incluida en la versión impresa del folleto guía. Por favor, dirígete a la Guía de Usuario del Psiphon [195] [3].

El **Peacefire** mantiene un gran número de *proxies* [181] públicos basados en la web, los cuales pueden ser seguros e inseguros dependiendo de como accedes a ellos. Cuando utilices el proxy *Peacefire* [193], debes ingresar la dirección *HTTPS* [190]con el fin de tener una conexión segura entre tú y el proxy. Los nuevos proxies se anuncian a través de una larga lista de correo de manera regular. Pueden inscribirte para recibir actualizaciones en el sito web de Peacefire [206] [11].

Mansour: ¡Excelente! De modo que nuestro Proveedor de Servicio de Internet (ISP) no puede ver lo que estamos hacienda cuando utilizo un servidor proxy, ¿correcto?

Magda: En tanto que utilicemos un proxy seguro, y le demos unos minutos a cada 'advertencia de certificado de seguridad' que pueda aparecer, entonces si, es verdad. Ten en cuenta que los proxies inseguros te permitirán evadir la mayoría de los filtros de Internet, pero también le permitirán a tu Proveedor de Servicio de Internet (ISP) fisgonear en tu conexión, incluyendo la localización de las páginas que estas visitando.

Lecturas Adicionales

- Dirígete a los capítulos Vigilancia y Observación en Internet [207] y Evasión de la Censura [208] del libro Seguridad Digital y Privacidad para Defensores de los Derechos Humanos [30] [12].
- El sitio web de los Manuales de Software Libre y de Código Abierto (FOSS) también contiene una guía sobre Cómo Evadir la Censura en Internet [209] [13].
- El Sitio web del Proyecto Sesawe [210] [14], mantiene un lista de herramientas de evasión y de información diversa sobre filtrado en Internet.
- El Wiki acerca de Censura en Internet [211] [15], escrita por Freerk se halla disponible en Inglés, Alemán y Español.
- El CitizenLab ha producido la Guía General para Evadir la Censura en Internet [212] [16], la cual está siendo traducida al Birmano, Inglés, Francés, Ruso, Español y Urdu.
- Reporteros Sin Fronteras ha lanzado una segunda edición de su Guía para escritores de bitácoras (Bloggers) y Ciberdisidentes [213] [17], el cual está disponible en Árabe, Birmano, Chino, Inglés, Farsi, Francés, Ruso y Español.
- Ethan Zuckerman de Global Voices Online ha publicado una guía útil de Añadir material a una Bitácora (Blog) de manera anónima con Wordpress y Tor [214] [18].

Referencias

[1] www.opennet.net [215]
[2] www.rsf.org [216]
[3] https://sesawe.net/Using-psiphon-2.html [195]
[4] www.psiphon.ca [217]
[5] https://sesawe.net/Anchor-Free-Hotspot-Shield.html [198]
[6] www.hotspotshield.com [218]
[7] www.your-freedom.net/index.php?id=3 [200]
[8] www.your-freedom.net/index.php?id=170 [219]
[9] www.your-freedom.net [220]
[10] https://sesawe.net/Using-Your-Freedom.html [221]
[11] www.peacefire.org [222]
[12] www.frontlinedefenders.org/manual/en/esecman/ [30]
[13] www.flossmanuals.net/CircumventionTools [223]
[14] https://sesawe.net/ [224]
[15] www.en.cship.org/wiki/Main_Page [225]
[16] www.civisec.org/sites/securitybkp.ngoinabox.org/themes/civisec/guides/ev... [212]
[17] www.rsf.org/rubrique.php3?id_rubrique=542 [213]
[18] http://advocacy.globalvoicesonline.org/tools/guide [226]

9. Protegerte a ti mismo y a tus datos cuando utilizas sitios de redes sociales

Las comunidades en línea han existido desde la invención de la Internet. Primero habían tablones de anuncios y listas de correo electrónico, las cuales le dieron a las personas alrededor del mundo la oportunidad de conectarse, comunicarse y compartir información sobre temas particulares. Hoy en día, los sitios web de redes sociales han expandido enormemente el rango de posibles interacciones, permitiéndote compartir mensajes, imágenes, archivos e incluso información actualizada al minuto acerca de lo que estas haciendo y donde estas. Estas funciones no son nuevas o únicas – cualquiera de estas acciones pueden también ser ejecutadas por medio de la Internet sin tener que unirse a un sitio de redes sociales.

Aunque estas redes pueden ser muy útiles, y promueven la interacción social tanto en línea como fuera de ella, cuando las utilizas podrías estar poniendo a disposición información para personas que quieran hacer mal uso de ella. Piensa en las redes sociales como si fueran una enorme fiesta. Ahí hay personas que conoces, así como algunas que no conoces en absoluto. Imagina caminar a través de la fiesta con todos tus detalles personales, y explicaciones de lo que piensas, actualizadas al minuto de lo que estas pensando, escrito en un gran aviso adherido a tu espalda de modo que todos puedan leerlo sin que incluso lo sepas. ¿Realmente deseas que todos sepan todo sobre ti?

Recuerda que los sitios de redes sociales son propiedad de empresas privadas, y que estas hacen dinero recolectando datos sobre personas y vendiéndolos, especialmente a terceros anunciantes. Cuando ingresas al sitio de una red social, estas dejando atrás las libertades de la Internet y estás ingresando a una red que está gobernada y regida por los dueños del sitio. Las configuraciones de privacidad sólo suponen tu protección de otros miembros de la red social, pero no protegen tus datos de los propietarios del servicio. Básicamente estas cediendo todos tus datos a los propietarios y confiándoselos a ellos.

Si trabajas con información y tópicos sensibles, y estás interesado en utilizar los servicios de las redes sociales, es importante que seas consciente de los problemas de privacidad y seguridad que estás generan. Los defensores de los

derechos humanos son particularmente vulnerables a los peligros de los sitos de redes sociales y necesitan ser extremadamente cuidadosos sobre la información que revelan sobre sí mismos y sobre las personas con las que trabajan.

Antes de utilizar cualquier sitio de redes sociales es importante entender cómo te hacen vulnerable, y luego dar pasos para protegerte a ti mismo y a las personas con las que trabajas. Esta guía te ayudará a entender las consecuencias de seguridad derivadas del uso de sitios de redes sociales.

Contexto:

Mansour y Magda son defensores de derechos humanos en el norte de África. Ellos están organizando una marcha, que tendrá lugar en el centro de una gran ciudad. Ellos quiere utilizar Facebook para publicitar el evento. Están preocupados de que las autoridades pudieran estar avisadas y que cualquiera que muestre interés pudiera ser rastreado. Planean utilizar Twitter durante la marcha para publicar actualizaciones del progreso de la marcha. Pero, ¿que pasaría si la policía pudiera detectar los mensajes, y desplegar escuadrones para interceptar a los marchantes? Mansour y Magda planifican cómo compartir fotos y videos de la marcha sin revelar las identidades de las personas, porque les preocupa que los participantes puedan sufrir persecución.

No te alentamos a dejar del todo de utilizar las herramientas de las redes sociales. Sin embargo, debes tomar las medidas de seguridad pertinentes, de modo que puedas utilizar estas herramientas sin hacer que tu o alguien más sean vulnerables.

¿Qué aprenderás en este capítulo?

- Como las redes sociales facilitan la revelación no intencional de información sensible
- Como salvaguardar información propia y ajena cuando utilizas los sitios de redes sociales

Consejos generales sobre el uso de las herramientas de redes sociales

- **Siempre hazte las preguntas:**
    - ¿Quién puede acceder a la información que estoy colocando en línea?
    - ¿Quién controla y posee la información que coloco en un sitio de redes sociales?
    - ¿Qué información propia están transmitiendo mis contactos a otras personas?
    - ¿Les importa a mis contactos si comparto información sobre ellos con otras personas?
    - ¿Confío en todas las personas con las que estoy conectado?
- Asegúrate siempre de utilizar **contraseñas seguras** para acceder a las redes sociales. Si otra persona se mete en tu cuenta, estará accediendo a mucha información sobre ti y sobre cualquiera con quien estés conectado a través de la red social. Cambia tus contraseñas regularmente como si fuera un asunto de rutina. Consulta Capitulo 3. Crear y mantener contraseñas seguras [227] para mayor información.
- Asegúrate de que entiendes la **configuración de privacidad** por defecto ofrecida por el sito de redes sociales, y cómo cambiarlos.
- Evalúa utilizar **cuentas/identidades separadas**, o talvez diferentes seudónimos, para diferentes campañas y actividades. Recuerda que la clave para utilizar una red de manera segura es siendo capaz de confiar en sus miembros. Las cuentas separadas pueden ser una buena manera de garantizar que dicha confianza sea posible.
- Se cuidadoso cuando accedas a tu cuenta en la red social en espacios públicos con Internet. **Borra tu contraseña e historial de navegación** cuando utilices un navegador en una máquina pública. Consulta Capítulo 6. Destruir información sensible [227].
- **Accede a los sitios de redes sociales utilizando https://** para salvaguardar tu nombre de usuario, contraseña y otra información que coloques. El utilizar https:// en vez de http:// añade otra capa de seguridad por medio del cifrado del tráfico de tu navegador al sitio de tu red social. Consulta Capítulo 8. Mantenerse en el anonimato y evadir la censura en Internet [147].
- Cuídate de no poner demasiada información en **tus actualizaciones de estado** – incluso si confías en las personas en tus redes. Es fácil para cualquiera copiar tu información.
- La mayoría de redes sociales te permite integrar información con otras redes sociales. Por ejemplo puedes publicar una actualización en tu cuenta de Twitter y hacer también que esta automáticamente se publique en tu cuenta de Facebook. Se especialmente **cuidadoso cuando integres las cuentas de tus redes sociales**! Podrías ser anónimo en un sitio, pero estar expuesto cuando utilices otro.
- Se cauteloso sobre cuan seguro está tu contenido en un sito de red social. **Nunca confíes en un sitio de red social como receptor primario para tu contenido** o información. Es muy fácil para los gobiernos bloquear el acceso a un sitio de red social dentro de sus límites si de pronto encuentran su contenido censurable. Los administradores de un sitio de red social podrían también decidir retirar ellos mismos el contenido censurable, en vez de afrontar la censura

dentro de un país en particular.

Publicar detalles personales

Los sitios de redes sociales te requieren una gran cantidad de datos personales para hacer más fácil a otros usuarios el ubicarte y conectarse contigo. Talvez la más grande vulnerabilidad que esto crea a los usuarios de estos sitios es la posibilidad de un fraude de identidad, el cual es crecientemente común. Además, cuanto mayor información propia reveles en línea, más fácil será para las autoridades identificarte y vigilar tus actividades. Las actividades en línea de activistas de la diáspora de algunos países ha conducido a las autoridades a convertir en objetivos a sus familiares residentes en su tierra natal.

Pregúntate: ¿es necesario publicar la siguiente información en línea?

- fechas de nacimiento
- números telefónicos de contacto
- direcciones
- detalles de miembros de la familia
- orientación sexual
- historial de educación y empleo

Mansour: Nuestro buen amigo acaba de ser expulsado en la frontera y fue colocado en un vuelo de regreso a su país. El oficial de frontera le preguntó si había escrito un artículo criticando al régimen. ¿Cómo supieron de ello cuando este no había sido publicado en este país?

Magda: La agencia de fronteras esta actualmente buscando nombres de personas en la Internet a medida que realizan sus tramites. Probablemente vieron el CV que ella publicó en su cuenta de Facebook.

Amigos, seguidores y contactos

La primera cosa que harás después de completar tus detalles personales en la solicitud de cualquier red social es establecer conexiones a otras personas. Presumiblemente estos contactos son personas que conoces y en quienes confías – pero podrías también estar conectándote a una comunidad en línea de personas afines que tu nunca has conocido. Lo más importante que debes entender es que información le estas permitiendo tener a esta comunidad en línea.

Cuando utilices una cuenta de red social tal como Facebook, donde se mantiene mucha información personal, evalúa conectarte sólo con personas que conoces y en quienes confías; y que sabes que no utilizarán la información que publicas de mala manera.

Mansour: Wow, desde la protesta he tenido docenas de pedidos de personas que quieren ser mis amigos en Facebook. Esta es una forma fabulosa para expandir nuestro alcance y permitir a las personas saber sobre ¡protestas futuras!

Magda: ¡Espera! ¿Conoces a todas esas personas? ¿Cómo sabemos que no son la policía o las autoridades que están tratando de obtener información sobre las próximas protestas?

Actualizaciones de estado

En el Twitter y en Facebook y en redes similares, la actualización de estado responde a las preguntas: ¿Qué estoy haciendo ahora? ¿qué esta pasando? La cosa más importante que debes entender sobre la actualización del estado es quién puede verla realmente. La configuración por defecto para la actualización del estado en la mayoría de las aplicaciones de red social es que cualquiera en la Internet puede verla. Si sólo quieres que tus contactos vean tus actualizaciones, necesitas comunicarle a la aplicación de red social que mantenga tus actualizaciones escondidas del resto.

Para hacer esto en Twitter, busca “Proteger tus Tweets”. En el Facebook, cambia tu configuración para compartir tus actualizaciones a “Sólo Amigos”. Incluso si cambias a dicha configuración, considera cuan fácil es para tus seguidores y amigos re-publicar tu información. Acuerda con tu red de amigos un enfoque común para trasladar la información publicada de sus cuentas de red social. También debes pensar acerca de que podrías revelar sobre tus amigos que ellos no quisieran que supieran otros; es importante ser perceptivo acerca de esto, y pedirle a otros ser perceptivos acerca de lo que revelan sobre ti.

Han habido muchos incidentes en los cuales la información incluida en las actualizaciones de estado han sido utilizadas contra las personas. Profesores en los EE.UU. han sido despedidos después de publicar actualizaciones sobre cómo se sentían acerca de sus estudiantes; otros empleados han perdido sus trabajos por publicar acerca de sus empleadores. Ello es algo de lo que casi todos necesitan ser cuidadosos.

Compartir contenido de Internet

Es fácil compartir un enlace a un sitio web y llamar la atención de tu amigo. Pero, ¿quiénes más estarán prestando atención, y que clase de reacción tendrán? Si dices que te gusta un sitio que en cierta forma esta relacionado a derrocar

un régimen represivo, dicho régimen podrían tomar interés y entonces tenerte en la mira.

Si quieres que tus contactos sean las únicas personas que vean las cosas que compartes o marcas como interesantes, asegúrate de revisar tu configuración de privacidad.

Revelar tu ubicación

La mayoría de los sitios de redes sociales mostrarán tu ubicación si dichos datos están disponibles. Esta función es proporcionada generalmente cuando utilizas un teléfono con capacidad GPS para interactuar con una red social, pero no asumas que no es posible si no estás conectado desde un teléfono móvil. La red a la que está conectada tu computadora puede también proveer datos de ubicación. La manera de estar a salvo de esto es verificar dos veces tu configuración.

Se especialmente cuidadoso sobre las opciones de ubicación en los sitios de intercambio de fotos y videos. No asumas simplemente que estos no están compartiendo tu ubicación: verifica dos veces tu configuración para estar seguro.

Consulta también Sobre Privacidad de la Ubicación, y Cómo Evitar Perderla para Siempre [228] en el sitio web de la Electronic Frontier Foundation.

Compartir videos/fotos

Fotos y videos pueden muy fácilmente revelar las identidades de las personas. Es importante que tengas el consentimiento de los sujetos que se hallen en cualquier foto o video que publiques. Si estás publicando la imagen de otra persona, se consciente de cómo podrías estar poniendo en peligro su privacidad. Nunca publiques un video o foto de alguien sin tener primero su consentimiento.

Los fotos y videos también pueden sin intención revelar mucha información. Muchas cámaras insertarán datos ocultos (rótulos de metadatos), que revelan la fecha, hora y ubicación de la foto, tipo de cámara, etc. Los sitios de intercambio de foto y video podrían publicar esta información cuando subes contenido a sus sitios.

Mansour: ¿Sabías que las autoridades en Myanmar fueron capaces de identificar muchos de los sacerdotes involucrados en las protestas de la revolución del azafrán a través de videos y fotos publicadas internacionalmente? Cualquiera que pudieron identificar fue puesto en la cárcel.

Magda: Si, necesitamos asegurarnos de que ningún rostro aparezca en las fotos de la demostración que publiquemos en línea. Debemos difuminar los rostros o utilizar fotos en las que todos se muestren de espaldas.

Charlas instantáneas

Muchos sitios de redes sociales tiene herramientas que te permiten tener discusiones con tus amigos en tiempo real. Estos operan como la Mensajería Instantánea y son una de las formas más inseguras de comunicarse en la Internet. Con el fin de asegurarte de que tus charlas son seguras, tu y tus amigos necesitan iniciar una sesión en tus cuentas de redes sociales utilizando https://, o utilizando un cliente para tus charlas, tal como el Pidgin con un programa añadido Off-the-record, que utiliza cifrado. Lee la Guía Práctica de 'Pidgin – mensajería instantánea segura'.

Unirse/crear grupos, eventos y comunidades

¿Qué información le estás dando a las personas si te unes a un grupo o comunidad? ¿Qué dice este hecho sobre ti? Por otro lado, ¿qué es lo que las personas anuncian al mundo si se unen a un grupo o comunidad que has creado? ¿Cómo estas poniendo en riesgo a las personas?

Cuando te unes a una comunidad o grupo en línea esto revela algo acerca tuyo a otros. En general, las personas podrían asumir que tu apoyas o estás de acuerdo con lo que el grupo esta diciendo o haciendo, lo cual podría hacerte vulnerable si estás siendo visto como alineado a un grupos políticos particulares, por ejemplo. Por otro lado, si te unes a un grupo con un gran número de miembros que no conoces, entonces ello podría poner en peligro algunas opciones de privacidad o seguridad que has empleado en tu cuenta, por tanto reflexiona acerca de que información estás entregando antes de unirte. ¿Estas utilizando tu foto y nombre real de modo que extraños puedan identificarte?

De modo alternativo, si estableces un grupo y las personas eligen unirse a este, ¿qué mensaje están enviando al mundo al hacerlo? Por ejemplo, tal vez sea un grupo de apoyo a gays y lesbianas el que has formado para ayudar a las personas, pero al unirse al mismo las personas se están identificando abiertamente como homosexuales o amistosos con ellos, lo cual podría generarles riesgos en el mundo real.

Monsour: Nuestros amigos en Siria no pueden venir a nuestra conferencia en Estambul porque se unieron a un grupo en Facebook “Fin a la Prohibición de Viaje en Siria”, y ahora tienen impuesta una prohibición de viaje.

Magda: ¿Podemos crear un grupo llamado “Viva la Prohibición de Viaje en Siria”, ¿hacemos que se unan y vemos si se les levantan sus prohibiciones?

Herramientas de redes sociales

Facebook

Facebook se ha convertido en el más grande sitio de redes sociales en el mundo. Si deseas contactar personas a través de una plataforma de red social, es probable que estos estén utilizando Facebook. Ello significa que utilizar Facebook es incluso más peligroso que utilizar otros sitios, dado que es accesible universalmente ello implica que casi cualquiera puede mirar la información que publicas ahí.

El fundador de Facebook, Mark Zuckerberg, ha declarado públicamente que la “privacidad en línea esta muerta” y es verdad que la privacidad en Facebook puede ser difícil de alcanzar. Aunque hayas revisado las confusas características que aparecen para garantizarte que sólo tus 'amigos' adscritos tengan acceso a tu información, esta todavía puede ser accesible a extraños por medio de una simple búsqueda, o a desarrolladores que hayan configurado una de las múltiples aplicaciones y juegos que las personas utilizan en el sitio.

Es importante notar que una vez que has configurado una cuenta de usuario con Facebook, no podrás borrarla. Facebook 'desactivará' tu cuenta a solicitud tuya pero permitirá 'reactivarla' con toda tu información y configuración intactos cuando quieras. Tus datos nunca se borran de Facebook.

De http://www.facebook.com/terms [229] - “*Para el contenido protegido por derechos de propiedad intelectual, como fotografías y vídeos ('contenido de PI'), nos concedes específicamente el siguiente permiso, de acuerdo con tu configuración de privacidad [230] y aplicación [231]: nos concedes una licencia no exclusiva, transferible, con posibilidad de ser sub-otorgada, sin regalías, aplicable globalmente, para utilizar cualquier contenido de PI que publiques en Facebook o en conexión con Facebook ('licencia de PI'). Esta licencia de PI finaliza cuando eliminas tu contenido de PI o tu cuenta (a menos que el contenido se haya compartido con terceros y éstos no lo hayan eliminado)*.” En otras palabras, Facebook es propietario de todos los datos que publiques en este, y puede utilizarlos como quiera.

El Departamento de Seguridad Nacional de los Estados Unidos de América vigila Facebook y otros sitios de redes sociales y es altamente probable que otros gobiernos hagan lo mismo.

Consejos sobre Facebook:

- Verifica dos veces tu configuración de privacidad en Facebook. Como consecuencia de la presión pública y del crecimiento sin precedente de su red, sus políticas de privacidad están cambiando permanentemente.
- El acto de 'hacer amistades' en Facebook significa que estás estableciendo una conexión directa con otros usuarios y les estas permitiendo ver tu información y tus actividades en Facebook. Es una buena práctica 'hacer amistad' en Facebook sólo con personas de quienes tengas razones reales para confiar.
- Evalúa desactivar tu cuenta cada vez que cierres tu sesión en esta. Ello significa que tu cuenta estará cerrada y nadie puede acceder a ella cuando no estás en línea. Puedes reactivar la cuenta cuando inicies sesión y todas tus características se mantendrán sin cambio.

Un buen lugar para empezar a comprender tu configuración de privacidad en Facebook es en su página 'Control de lo que Compartes' http://www.facebook.com/privacy/explanation.php [232]

Twitter

Funciones: Actualización de Estatus

Twitter empezó como un servicio para publicar actualizaciones desde un teléfono móvil a la Internet, por ello el límite de 140 caracteres. Esta también es la razón por la que es descrito como un 'SMS para la Internet'. En Twitter, tu 'sigues' a otros usuarios que te interesan, en vez de personas a las que conoces en realidad. Esto significa que tus seguidores no son necesariamente tus amigos y hace que el establecimiento de culpabilidad por asociación sea un poco más difícil. Ello también hace más fácil que las personas utilicen falsas identidades o escondan sus propias identidades.

Twitter establece en sus Términos de servicio: “*Este permiso autoriza a Twitter para poner tus Tweets a disposición del resto del mundo y permitir que otros hagan lo mismo. Pero lo que es tuyo es tuyo. Tú eres dueño de tu propio contenido*.” (extraído de http://twitter.com/terms [233])

Aunque Twitter es un sitio web, muchas personas interactúan con y administran Twitter a través de aplicaciones de escritorio conocidas como clientes Twitter. Si utilizas un cliente Twitter debes asegurarte que se está conectando al sitio de manera segura.

El Departamento de Seguridad Nacional de los Estados Unidos de América vigila Twitter y otras redes sociales y es altamente probable que otros gobiernos hagan lo mismo.

Consejos sobre Twitter

- “Lo que digas en Twitter se verá alrededor del mundo instantáneamente. ¡Eres lo que Twitteas!” (extraido de http://twitter.com/terms [233])
- Recuerda, cualquier mensaje en Twitter va a la línea de tiempo pública, lo que significa que es accesible a cualquiera, no sólo a tus seguidores. Evalúa proteger tus mensajes si publicas información sensible. El proteger tus

tweets significa que sólo tus seguidores pueden verlos: sin embargo, recuerda que los seguidores son libres de volver a publicar tus tweets y hacerlos públicos.

- Considera utilizar un seudónimo o una falsa identidad si estás twitteando críticas a funcionarios o gobiernos.

YouTube

Funciones: compartir video, compartir contenido de Internet

YouTube es propiedad de Google. YouTube es excelente para poner tu video a disposición de sus miles de millones de usuarios. Sin embargo, si la gente de Google considera censurable el contenido de tu video, lo borrarán. Esto implica que YouTube no es un buen lugar para mantener a salvo tu video. Google es conocido por ceder a la presión para retirar contenido de YouTube con el fin de evitar que el sitio sea censurado. De modo que si quieres que las personas vena tu video, coloca una copia de este en YouTube – sólo no pongas tu única copia en YouTube como almacenamiento seguro.

Google registrará tanto los datos de nombres de usuario como aquellos de ubicación por cada vídeo subido y visualizado. Esto podría ser potencialmente utilizado para rastrear personas.

El contenido de tu publicación en YouTube se mantiene como tuyo; al colocarlo en YouTube le das a Google una licencia para distribuir dicho contenido.

Hasta septiembre de 2010, YouTube estaba prohibido en China, Irán, Libia, Tunez y Turkmenistán.

Consejos sobre YouTube:

- Nunca publiques un vídeo de una persona sin su consentimiento. E incluso con su consentimiento, intenta pensar en cualquier posible repercusión antes de publicarlo.
- Siempre conserva una copia de seguridad de cualquier vídeo que compartas a través de Google/YouTube.
- Utiliza la configuración de privado con el fin de compartir vídeo sólo con personas específicas.

Flickr

Funciones: compartir foto/vídeo, compartir contenido de Internet

Flickr es propiedad de Yahoo!

El contenido publicado en Flickr permanece como tuyo, al cual puede atribuirle diversas licencias de creative commons o de derechos de autor. Le concedes a Yahoo una licencia para distribuir tus fotos o vídeos al remitir contenido.

Debido a la variada atribución de licencias, Flickr es excelente para encontrar imágenes para ser utilizadas en campañas y como una fuente para intercambiar imágenes con colegas, aliados y miembros de tus redes.

Consejos sobre Flickr

- Verifica que Flickr no este también mostrando información oculta registrada por tu cámara digital (metadatos); estos pueden ser fecha, hora, ubicación GPS, modelo de la cámara, etc.
- Nunca compartas la foto de una persona en Flickr sin su consentimiento, y está seguro que las persona/s en cualquiera de las fotos este de acuerdo con el tipo de licencia que has elegido asignar a su imagen.

El Departamento de Seguridad Nacional de los Estados Unidos de América vigila Flickr y otros sitios de redes sociales y es altamente probable que otros gobiernos también lo hagan.

Nota Final: Herramientas Alternativas

Los sitios web listados en este capítulo son las más populares y ampliamente utilizadas herramientas de redes sociales. La ofensiva de los gobiernos pondrá primero en la mira a estos sitios y los bloqueará. Dado que todas estas herramientas pertenecen a compañías privadas, estas cederán a las presiones gubernamentales y censurarán cuando sea necesario. Podría valer la pena mirar sitos alternativos a estos, tales como Diaspora (http://joindiaspora.com [234]) y Crabgrass (http://we.riseup.net [235]) los cuales han sido diseñados pensando en la seguridad digital y en el activismo.

10. Utilizar los teléfonos móviles de la manera más segura posible

Los teléfonos móviles son una parte integral de nuestras comunicaciones diarias. Todos los teléfonos móviles tiene la capacidad para servicios de mensajería de voz y de texto simple. Su pequeño tamaño, relativamente bajo costo y muchos

usos hacen de estos dispositivos invaluables para los defensores de derechos que cada día los utilizan más para propósitos de comunicación y organización.

Recientemente, se han puesto a disposición dispositivos móviles con muchas más funciones. Estos pueden contar con GPS, capacidad multimedia (registro de foto, video y audio y a veces su transmisión), procesamiento de datos y acceso a la Internet. Sin embargo, la forma en la que la red móvil opera, y su infraestructura, son esencialmente distintos a aquellos como funciona la Internet. Esto crea retos adicionales a la seguridad, y riesgos para la privacidad de los usuarios y la integridad de su información y comunicaciones.

Contexto

Borna y su hijo Delir son trabajadores de una fábrica, y están colaborando con la creación de un sindicato de trabajadores. Su empeño se enfrenta a la resistencia de los dueños de la fábrica, los cuales tienen buenas relacionas con el gobierno local. El supervisor de Borna le ha advertido que podría estar bajo la atenta mirada de la administración, y que debe tener cuidado de con quien habla. Borna ha comprado un teléfono móvil para su sindicato de trabajadores. Delir está ayudando a su padre a utilizar su nuevo teléfono móvil de manera segura para algunas de sus actividades de organización.

¿Qué puedes aprender de este capitulo?

- Por qué la comunicación y el almacenamiento de datos en teléfonos móviles no es segura.
- Que pasos puedes dar para incrementar la seguridad en el uso de teléfonos móviles.
- De que manera puedes minimizar las probabilidades de ser espiado o rastreado a través de tu teléfono móvil.
- De que manera puedes maximizar tus probabilidades de mantenerte en el anonimato al momento de utilizar tu teléfono móvil.

10.1 Dispositivos móviles y seguridad

Necesitamos tomar decisiones informadas cuando utilizamos teléfonos móviles, con el fin de protegernos a nosotros mismos, a nuestros contactos y nuestros datos. La manera en la que las redes y la infraestructura telefónica funcionan pueden afectar significativamente la capacidad de los usuarios para mantener privadas y seguras la información y las comunicaciones.

- Las redes de telefonía móvil son redes privadas administradas por entidades comerciales, las cuales pueden estar bajo el control monopólico del gobierno. La entidad comercial (o gubernamental), tiene prácticamente acceso ilimitado a la información y a las comunicaciones de sus clientes, así como la capacidad para interceptar llamadas, mensajes de texto, y vigilar la ubicación de cada aparato (y por tanto de sus usuarios).

- Los Sistemas Operativos en sí, utilizados en aparatos móviles son hechos a pedido o configurados por los fabricantes de teléfonos de acuerdo a las especificaciones de varios proveedores de servicios y para su uso en las propias redes de esas compañías. En consecuencia, el Sistema Operativo (OS) puede incluir características escondidas que permitan una mejor vigilancia por parte de los proveedores de servicio de cualquier dispositivo en particular.

- El número de las funciones disponibles en los teléfonos móviles ha crecido en años recientes. Los teléfonos móviles modernos son de hecho minicomputadoras portátiles conectadas a Internet con funciones de teléfono móvil.

Con el fin de determinar que aspectos de tus comunicaciones necesitan estar más protegidos, podría ser de ayuda hacerte a ti mismo algunas interrogantes: ¿Cuál es el contenido de tus llamadas y de tus mensajes de texto?, ¿Con quién te comunicas, y cuándo?, ¿De donde estás llamando? La información es vulnerable de distintas maneras:

- **La información es vulnerable cuando se envía desde un teléfono móvil**
  Ejemplo: Cada uno de los proveedores de telefonía móvil tiene acceso completo a todos los mensajes de texto y voz enviados a través de su red. Los proveedores telefónicos en la mayoría de países están legalmente obligados a mantener registros de todas las comunicaciones. En algunos países los proveedores telefónicos están bajo el control monopólico del gobierno. Las comunicaciones de voz y texto también pueden ser intervenidas por terceros en las proximidades al teléfono móvil, utilizando equipo de bajo precio.

- **La información es vulnerable al interior de los teléfonos tanto del emisor como del receptor**
  Ejemplo: Los teléfonos móviles pueden almacenar toda clase de datos: historial de llamadas, mensajes de texto enviados y recibidos, información de libretas de direcciones, fotos, video clips, archivos de texto. Estos datos pueden revelar tu red de contactos, e información personal sobre ti y tus colegas. Asegurar esta información es difícil, incluso – en algunos teléfonos – imposible. Los teléfonos modernos son computadoras de bolsillo. Con más funciones el riesgo se hace mayor. Además, los teléfonos que se conectan a la Internet también están sujetos a las inseguridades de las computadoras y de la Internet.

- **Los teléfonos dan información acerca de su ubicación**
  Ejemplo: Como parte de su operación normal, cada teléfono móvil automáticamente y de manera regular informa al proveedor del servicio telefónico donde está en determinado momento. Es más, muchos teléfonos hoy en día tienen funciones de GPS, y esta información precisa sobre la ubicación podría ser incorporada en otros tipos de datos tales

como fotos, el servicio de mensajes cortos (SMS) y en solicitudes de Internet que son enviadas desde el teléfono.

La evolución de la tecnología trae más características, pero también más riesgos.

Borna: Hijo, he decidido sólo utilizar este teléfono móvil para planificar nuestras reuniones de ahora en adelante, porque creo que podrían estar interviniendo el teléfono de la fábrica, y quizás incluso el de la casa.

Delir: Padre, es bueno que por fin tengas un teléfono móvil, pero ¿sabes qué es lo que puede y no puede hacer?

Borna: Claro: ¡Es un teléfono! Puedes llamar a alguien, hablar con ellos, ellos responden. Puedes hacerlo desde cualquier lugar en que te encuentres. Y, desde el puedo enviar pequeños mensajes a otros, o a ti, y estos aparecerán en tu teléfono.

Delir: Todo ello es cierto, pero eso no es todo. En estos días, hay muchas cosas que puedes hacer con estos dispositivos. Pero hablemos de algunos riesgos y precauciones de seguridad, especialmente si crees que alguien podría estar interesado en saber con quien te estas comunicando, y que estas diciendo.

Las siguientes secciones examinan varios pasos simples que puedes dar para reducir la posibilidad de amenazas a tu seguridad que surgen del uso de dispositivos móviles.

10.2 Movilidad y vulnerabilidad de la información

Las personas a menudo portan teléfonos móviles que contienen información sensible. Historial de comunicaciones, mensajes de texto y de voz, libretas de direcciones, calendarios, fotos y muchas otras funciones útiles de los teléfonos pueden convertirse en altamente peligrosas si el teléfono o los datos se pierden o son robados. Es vital estar conciente de la información que se almacena, tanto en forma activa como pasiva, en tu teléfono móvil. La información almacenada en un teléfono podría implicar a la persona que utiliza el teléfono así como a todos los que se hallan en su libreta de direcciones, su bandeja de entrada de mensajes, su álbum de fotografías, etc.

Los teléfonos móviles que se conecta a la Internet también están sujetos a los riesgos y vulnerabilidades asociadas con la Internet y las computadoras, como se abordó en los otros capítulos de este documento relativo a la seguridad de la información, el anonimato, la recuperación de la información, la perdida, el robo y la intercepción.

Con el fin de reducir algunos de estos riesgos de seguridad, los usuarios deben ser conscientes del potencial de inseguridad de sus teléfonos, así como de sus opciones de configuración. Una vez que sepas cuales podrían ser los posibles problemas, podrás poner salvaguardas y tomar medias preventivas.

Borna: Una ventaja de la telefonía móvil es que no sabrán donde son nuestras reuniones si las organizamos utilizando nuestros teléfonos móviles, mientras caminos en el mercado, en vez de utilizar los teléfonos fijos, donde podrían estar oyéndonos mientras hablamos.

Delir: Bueno, ¿Dijiste que ellos tenían conexiones en la compañía telefónica?

Borna: Alguien estuvo diciendo que estaban sobornando a técnicos en telefonía para obtener información.

Delir: Si firmaste la suscripción a este teléfono móvil utilizando tu identidad y tu dirección, este es atribuible a ti, y cada vez que realices una llamada, su registro está asociado a tu identidad y suscripción telefónica. ¿Lo contrataste utilizando tu identidad?

Borna: No, conseguí un teléfono de segunda mano en la tienda de tu tío; el me dijo que se aseguró que está limpio y es seguro utilizarlo. Además me ayudó a comprar uno de esos pequeños chips preparados que tu colocas en tu teléfono.

Delir: Si, ese chip se llama tarjeta SIM. La compañía telefónica rastrea cada llamada o transmisión con el número del teléfono, y con el número de identificación de la tarjeta SIM, Y el número de identificación del teléfono. De modo que si ellos conocen que número telefónico, O número de identificación del teléfono, O número de tarjeta SIM te pertenece, ellos podrían ser capaces de utilizar sus contactos para ver los patrones de uso de tu teléfono.

Borna: Y supongo que, entonces, ¿pueden escuchar mis conversaciones incluso en mi teléfono móvil?

Delir: En tu caso, y gracias al tío, tu teléfono no está registrado a tu nombre, y la tarjeta SIM tampoco está de alguna forma conectada a ti. Por tanto, incluso si rastrean donde están la tarjeta SIM y el teléfono no sabrán necesariamente que tu estás conectado a la tarjeta SIM, o al teléfono.

10.2.1 Buenas prácticas en seguridad telefónica

Como en el caso de otros dispositivos, la primera línea de defensa para la seguridad de la información en tu teléfono móvil es la protección física de tu teléfono móvil, y de su tarjeta SIM de ser tomadas o manipuladas.

- Mantén tu teléfono contigo siempre. Nunca lo dejes sin vigilancia. Evita mostrar tu teléfono en público.
- Siempre utiliza tus códigos de bloqueo de tu teléfono o los Números de Identificación Personal (PINs) y mantenlos en secreto (desconocidos para otros). Siempre cámbialos para que no sean lo que coloca el fabricante.
- Marca físicamente (dibuja en) la tarjeta SIM, tarjeta adicional de memoria, batería y teléfono con algo único y no rápidamente perceptible para un extraño (haz o pon una marca pequeña, dibujo, letras o números, o trata de utilizar un rotulador ultravioleta, el cual será invisible a la luz normal). Coloca etiquetas de seguridad impresas a prueba de manipulaciones o cinta adhesiva sobre las juntas del teléfono. Ello te ayudará a identificar fácilmente si alguno de estos objetos han sido manipulados o remplazados (por ejemplo, la etiqueta o la cinta adhesiva estará desalineada, o dejará un residuo perceptible).
- Asegúrate de ser consciente de la información que está almacenada en tu tarjeta SIM, en tarjetas adicionales y en la memoria de tu teléfono. No almacenes información sensible en el teléfono. Si necesitas almacenar dicha información, considera colocarla en tarjetas de memoria externas que puedan ser fácilmente desechadas en caso necesario – no coloques tales detalles en la memoria interna del teléfono.
- Protege tu tarjeta SIM y tu tarjeta adicional de memoria (si tu teléfono tiene una), pues estas podrían contener información sensible tales como detalles de contacto y mensajes SMS. Por ejemplo, asegúrate de no dejarlos en la tienda de reparaciones cuando tu teléfono esta siendo arreglado.
- Cuando te deshagas de tu teléfono asegúrate de que no estas entregando información que esté almacenada en este o en la tarjeta SIM o en la tarjeta de memoria (incluso si el teléfono o las tarjetas están rotas o han expirado). Deshacerte de las tarjetas SIM destruyéndolas físicamente podría ser la mejor opción. Si planeas obsequiar, vender o reutilizar tu teléfono asegúrate que toda la información sea eliminada.
- Considera utilizar únicamente comercios confiables de distribución y reparación de teléfonos. Ello reduce la vulnerabilidad de tu información cuando consigas teléfonos móviles de segundo uso o tengas que reparar tu teléfono. Ten presente que el comprar tu teléfono de un distribuidor autorizado pero elegido al azar – de este modo reducirás la posibilidad de que el teléfono esté específicamente preparado para ti con software espía preinstalado en el mismo.
- Haz regularmente copias de seguridad en tu computadora de la información que se encuentra en tu teléfono. Almacena la copia de seguridad de manera segura (dirígete la capítulo: 4. proteger los archivos sensibles en tu computadora). Esto te permitirá restaurar los datos si pierdes tu teléfono. Tener una copia de seguridad también te ayudará a recordar que información podrías estar en peligro (cuando tu teléfono se haya perdido o haya sido robado), de modo que puedas tomar las acciones pertinentes.
- El número de serie de 15 dígitos o número IMEI te ayuda a identificar tu teléfono y puede ser accedido tecleando *#06# en la mayoría de teléfonos, viendo detrás de la batería en tu teléfono o revisando las especificaciones del mismo. Toma nota de este número y mantenlo alejado de tu teléfono, pues este número podría ayudar a rastrear en caso sea robado y a probar la propiedad del mismo rápidamente.
- Pondera las ventajas y desventajas de registrar tu teléfono con el proveedor del servicio. Si informas que tu teléfono ha sido robado, el proveedor del servicio entonces será capaz de impedir el uso posterior de tu teléfono. Sin embargo, el registrarlo significa que el uso de tu teléfono está ligado a tu identidad.

10.2.2 Funciones básicas, capacidad de rastreo y anonimato

Con el fin de enviar o recibir llamadas o comunicaciones de cualquier tipo desde y hacia tu teléfono, la antenas de señal más cercanas son alertadas, sobre tu presencia, por tu teléfono móvil. Cómo resultado de tales alertas y comunicaciones el proveedor de servicios de red sabe exactamente la ubicación geográfica de tu teléfono móvil en un momento dado.

Borna: ¿Hay algo más que deba saber acerca de este teléfono?

Delir: Creo que si, pero eso depende de si realmente sospechas que están tratando de rastrearte.

Borna: No lo creo, pero ¿pueden hacerlo?

Delir: Bueno, si, si tienes tu teléfono encendido, Y si el técnico tiene acceso al tráfico de la red, Y si ellos saben que teléfono en el sistema es el tuyo.

Borna: Ello no ocurrirá debido a que simplemente no haré ninguna llamada desde mi teléfono una vez que llegue allí.

Delir: Eso no importa padre. En la medida que tengas el teléfono contigo, cargado y listo para usar, este mantendrá un registro de a donde vas, y se lo comunicará a las antenas de la red cercanas, simplemente porque tiene que hacerlo. De modo que en un momento dado, tu ubicación será aquella en algún punto entre las antenas más cercanas de la red telefónica.

Borna: Entonces ¿debo apagarlo hasta que llegue ahí?

Delir: Bueno, claro que lo mejor sería no llevarlo contigo. La siguiente mejor cosa que hacer es tenerlo apagado y sacarle la batería antes de ir, y no encenderlo hasta que regreses.

Borna: ¿Qué? ¿no es suficiente apagarlo?

Delir: Bueno, para mantenerte seguro, debes extraer la batería, y ahora te digo porque: este es un dispositivo de transmisión, y mientras la batería este conectada, existe una pequeña posibilidad de que de alguna manera alguien pueda encenderlo sin que lo sepas.

Sobre el Anonimato

Si estas llevando a cabo conversaciones telefónicas sensibles o enviando mensajes SMS sensibles, cuídate de la 'característica' de rastreo mencionada arriba ya que que se halla en todos los teléfonos móviles. Pondera el seguir los pasos siguientes:

- Cada vez que hagas llamadas hazlas de distintas ubicaciones, y elige ubicaciones que no se puedan asociar contigo.
- Mantén tu teléfono apagado, con la batería desconectada, ve a la ubicación elegida, enciende tu teléfono, comunícate, apaga tu teléfono y desconecta la batería antes de regresar. El hacer esto de manera habitual cada vez que tengas que hacer una llamada, significará que la red no pueda rastrear todos tus movimientos.
- Cambia a menudo de teléfonos y de tarjetas SIM. Rótalos entre amigos o con el mercado de segundo uso.
- Utiliza tarjetas SIM prepagadas no registradas si ello es posible en tu área. Evita pagar por un teléfono o tarjetas SIM utilizando una tarjeta de crédito, lo cual crearía una conexión entre estos objetos y tú.

Borna: Me estás diciendo que mi teléfono podría estar hablándoles a las antenas acerca de mi paradero, ¿incluso si se ve como si estuviera apagado?

Delir: Así es, y eso no es lo peor

Borna: ¿Qué?

Delir: Bueno, dicen que hay programas que pueden ser instalados en tu teléfono para secretamente encenderse a distancia y llamar a un número telefónico sin tu conocimiento. Entonces, al momento que empiezas tu reunión, este empezaría a actuar como un dispositivo de grabación y transmisión.

Borna: ¡No! ¿de veras?.

Delir: Bueno, es muy fácil de hacer desde el punto de vista tecnológico. Pero nada de ello puede suceder si la batería esta desconectada, de modo que estarás a salvo en este improbable caso.

Borna: Creo que simplemente no lo llevaré conmigo si quiero ser super cuidadoso. Pero me pregunto si debería de utilizarlo del todo.

Delir: Por favor, padre. Solías decirme que no me asustara de las nuevas cosas. Los teléfonos móviles son como ellas, tu sólo tienes que saber cuáles son los beneficios y los riesgos. Sólo se cuidadoso. Si conoces los riesgos, puedes dar los pasos necesarios para evitarlos.

Sobre escuchas secretas

Tu teléfono puede ser preparado para registrar y transmitir cualquier sonido dentro del rango de alcance de su micrófono sin tu conocimiento. Algunos teléfonos pueden ser encendidos de manera remota y puestos en acción de esta manera, aún cuando parezcan estar apagados.

- Nunca permitas que las personas de quienes desconfías tengan acceso físico a tu teléfono; esta es una manera común de instalar software espía en tu teléfono.
- Si estas conduciendo reuniones privadas e importantes, apaga tu teléfono y desconecta la batería. O no lleves el teléfono contigo si no puedes dejarlo donde pueda estar completamente a salvo.
- Asegúrate de que cualquier persona con la que te comuniques también emplee las acciones descritas aquí.
- Además, no olvides que utilizar un teléfono en público, o en lugares en los que no confías, te hacen vulnerable a las técnicas tradicionales de escucha secreta, o que te roben el teléfono.

Sobre intercepción de llamadas

Generalmente, el cifrado de las comunicaciones por voz (y por mensajes de texto) que viajan a través de la red de telefonía móvil es relativamente débil. Existen técnicas de bajo costo que pueden utilizar terceros para interceptar tus comunicaciones escritas, o para escuchar tus llamadas, si están en la proximidad de tu teléfono y pueden recibir

transmisiones desde el mismo. Y por su puesto, los proveedores de telefonía móvil tienen acceso a todas tus comunicaciones de voz y texto. Actualmente es costoso y/o de alguna manera técnicamente difícil cifrar las llamadas telefónicas de modo que incluso el proveedor de telefonía móvil no pueda escucharlas secretamente – sin embargo, se espera que estas herramientas pronto se vuelvan económicas. Para utilizar el cifrado primero tendrías que instalar una aplicación o programa de cifrado en tu teléfono, así como en el dispositivo de la persona con la cuál planeas comunicarte. Entonces utilizarías esta aplicación para enviar y recibir llamadas y/o mensajes cifrados. El software de cifrado actualmente sólo puede ser admitido en unos cuantos modelos llamados teléfonos 'inteligentes'.

Las conversaciones entre el Skype y los teléfonos móviles tampoco están cifrados, pues en algún punto, la señal se desplazará a la red móvil, donde el cifrado NO está en uso.

10.2.3 Comunicaciones textuales – SMS / Mensajes de texto

No debes confiar en los servicios de mensaje de textos para transmitir información sensible de manera segura. Los mensajes intercambiados son en texto simple lo que los hace inapropiados para transacciones confidenciales.

Borna: Que pasa si nunca hago llamadas desde mi teléfono móvil, y sólo envío y recibo estos pequeños mensajes. Ellos no pueden escuchar algo si nadie está diciendo nada, ¿y es muy rápido, no?

Delir: Espera. Estos mensajes también son fáciles de interceptar, y cualquiera con acceso al tráfico en la compañía telefónica, o incluso otras personas con el equipo correcto, pueden capturar y leer estos mensajes que se están moviendo alrededor de la red en texto simple, siendo guardados de una antena a la siguiente.

Borna: Eso realmente es tonto. ¿Qué debo hacer? ¿Escribir en código como hacíamos durante la guerra?

Delir: Bueno, a veces los zapatos más viejos son lo más cómodos.

El envío de mensajes SMS puede ser interceptado por el operador de servicio o por terceros con equipo de bajo costo. Dichos mensajes llevan los números telefónicos del emisor y del receptor así como el contenido del mensaje. Lo que es más, los mensajes SMS pueden ser fácilmente alterados o falsificados por terceros.

Piensa en establecer un sistema de código entre tu y tus correspondientes. Los códigos podrían hacer tu comunicación más segura y podrían proporcionar una forma adicional de confirmar la identidad de las personas con las que te estas comunicando. Los sistemas de código necesitan ser seguros y cambiar frecuentemente.

Los mensajes SMS están disponibles después de ser transmitidos:

- En muchos países, la legislación (u otras influencias) exigen a los proveedores de la red mantener un registro de largo plazo de todos los mensajes de texto enviados por sus clientes. En la mayoría de los casos los mensajes SMS son mantenidos por los proveedores para fines comerciales, contables o de litigio.
- Los mensajes en tu teléfono pueden ser fácilmente accedidos por cualquiera que consiga tu teléfono. Evalúa eliminar en seguida todos los mensajes recibidos y enviados.
- Algunos teléfonos tienen la facilidad de deshabilitar el registro del historial de llamadas telefónicas o de mensajes de texto. Ellos será especialmente útil para personas que realicen actividades más sensibles. También debes asegurarte de estar familiarizado con lo que tu teléfono es capaz de hacer. ¡Lee el manual!

10.2.4 Funciones más allá de la conversación y los mensajes

Los teléfonos móviles se están convirtiendo en dispositivos de computación móviles, con sus propios sistemas operativos y aplicaciones descargables que proveen diversos servicios a los usuarios. En consecuencia, los virus y el software espía han penetrado el mundo de la telefonía móvil. Los virus pueden ser sembrados en tu teléfono, o pueden venir empacados dentro de las aplicaciones, los tonos de llamada y mensajes multimedia que descargas de la Internet.

Mientras que los primeros modelos de teléfonos móviles tenían pocas o ninguna función de Internet, es no obstante importante observar las precauciones planteadas más abajo en todos los teléfonos, para estar absolutamente seguros de que su dispositivo no esta en peligro sin tu conocimiento. Algunas de estas precauciones podrían aplicarse sólo a los teléfonos inteligentes, pero es muy importante saber exactamente cuáles son las capacidades de tu teléfono, con el fin de tener certeza de que has tomado las las medidas apropiadas:

- No almacenes archivos y fotos confidenciales en tu teléfono móvil. Trasládalos, lo más pronto posible, a una ubicación segura, como se explica en el Capítulo 4, Proteger los archivos sensibles en tu computadora.
- Borra frecuentemente los registros de llamadas telefónicas, mensajes, ingreso de datos a tu libreta de direcciones, fotos, etc.

- Si utilizas tu teléfono para navegar en la Internet, sigue prácticas seguras similares a aquellas que utilizas cuando estas en la computadora (por ejemplo, siempre envía información a través de conexiones cifradas como HTTPS).
- Conecta tu teléfono a una computadora sólo si estás seguro que esta esta libre de software malicioso (malware). Consulta el Capítulo 1. Proteger tu computadora de software malicioso (malware) y piratas informáticos (hackers).
- No aceptes ni instales programas desconocidos y no verificados en tu teléfono, entre ellos tonos de llamada, fondos de pantalla, aplicaciones de java o cualquier otro que se origine en una fuente no deseada o inesperada. Estas pueden contener virus, software malicioso o programas espía.
- Observa el comportamiento y el funcionamiento de tu teléfono. Está atento a programas desconocidos y procesos en ejecución, mensajes extraños y funcionamiento irregular. Si no conoces o no utilizas algunas de las características y aplicaciones en tu teléfono, deshabilítalas o desinstálalas de ser posible.
- Se cauteloso cuando te conectes a los puntos de acceso WiFi que no ofrecen contraseñas, del mismo modo que lo serías cuando utilizas tu computadora y te conectas a puntos de acceso WiFi. El teléfono móvil es esencialmente como una computadora y por tanto comparte las vulnerabilidades e inseguridades que afectan a las computadoras y a la Internet.
- Asegúrate que estén apagados y deshabilitados en tu teléfono los canales de comunicación como el Infra Red (IR), Bluetooth y Wireless Internet (WiFi) si no los estás utilizando. Enciéndelos sólo cuando se requiera. Utilízalos sólo en situaciones y ubicaciones confiables. Evalúa no utilizar Bluetooth, pues es relativamente simple escuchar a escondidas en esta tipo de comunicaciones. En vez de ello, transfiere datos utilizando una conexión con cable desde el teléfono a audífonos de manos libres o a una computadora.

10.3 Lecturas Adicionales

- The Mobile Advocacy Toolkit [240] publicado por The Tactical Technology Collective. Entre otras cosas, este contiene descripciones detalladas y guías para la seguridad de teléfonos móviles [241] y también un amplio rango de otras herramientas y ejemplos relativos a su uso.
- Seguridad para Activistas - Un Manual Práctico de Seguridad para Activistas y Campañas [242].
- Guía de Teléfonos Móviles – Una guía corta, para activistas, para utilizar teléfonos móviles de forma segura [243].
- Guía de Seguridad Móvil para Ciudadanos Periodistas [244] publicada por MobileActive.org
- Una Breve Introducción a la Mensajería SMS Segura en MIDP - Guía del desarrollador de Nokia [245]
- Teléfonos utilizados como dispositivos espías [246]

11. Utilizar los teléfonos inteligentes de la manera más segura posible

En el ***Capítulo 10: Utilizar los teléfonos móviles de la manera más segura posible*** [247], conversamos sobre los retos de la seguridad al usar teléfonos móviles convencionales – incluidos los temas sobre los servicios de comunicación por voz y mensajes de textos (SMS/MSS). Estos teléfonos móviles primordialmente (sino exclusivamente) utilizan redes móviles para transferir llamadas y datos.

Actualmente, los avances tecnológicos han posibilitado que los teléfonos móviles contengan servicios y características similares a las computadoras de escritorio o portátiles. Estos teléfonos inteligentes ofrecen nuevas y variadas formas para comunicarse, capturar y difundir medios de comunicación. Para proveer estas nuevas funcionalidades, los teléfonos inteligentes no sólo utilizan la red móvil sino que se conectan a la internet a través de una conexión WiFi (similar a una computadora portátil en un café internet) o a través de un operador de red móvil.

Por lo tanto, aunque puedes realizar llamadas con un teléfono inteligente, es mejor considerar los teléfonos inteligentes como pequeños dispositivos de computación. Esto significa que el otro material didáctico de este kit de herramientas es relevante para el uso de tu teléfono inteligente así como para tu computadora.

Los teléfonos inteligentes usualmente son compatibles con una amplia gama de funcionalidades – navegación en internet, correo electrónico, mensajería de voz y de texto a través de la internet, capturar, guardar y transmitir audios, videos y fotos, habilitar redes sociales, juegos en línea con varios usuarios a la vez, banca en internet, y muchas otras actividades. Sin embargo muchas de estas herramientas y características implican nuevos temas de seguridad, o aumentan riesgos ya existentes.

Por ejemplo, algunos teléfonos inteligentes tienen incorporados una funcionalidad de geo-localización (*GPS* [248]), lo cual significa el teléfono le provee automáticamente al operador de red móvil tu ubicación exacta, como a las aplicaciones que utilizas en tu teléfono inteligente (tales como redes sociales, mapas, navegadores y otras aplicaciones). Como mencionamos anteriormente, el teléfono móvil ya transmite la información de tu ubicación al operador de la red móvil (como funciones normales del teléfono). Sin embargo, la funcionalidad adicional del GPS no sólo incrementa la precisión

de la información sobre tu ubicación, sino que además aumenta la cantidad de lugares en las que esta información puede ser distribuida.

Vale la pena revisar todos los riesgos asociados con los teléfonos móviles abordados en el ***Capítulo 10: Utilizar los teléfonos móviles de la manera más segura posible*** [247] ya que también son relevantes para el uso de teléfonos inteligentes. El ***Capítulo 10*** [247] abarca temas sobre escuchas ilegales, interceptación de SMS y/o llamadas teléfonicas, temas sobre las tarjetas SIM, y buenas prácticas.

En este capítulo abordaremos los retos adicionales a la seguridad que trae consigo el uso de los teléfonos inteligentes.

Bolsos, Billeteras, Télefonos Inteligentes

Intuitivamente comprendemos lo importante que es mantener seguros nuestros bolsos y billeteras, ya que sabemos que en ellos guardamos información sensible, y perderlos podría comprometer nuestra privacidad y seguridad. Las personas son menos conscientes de la cantidad de información personal que tienen en sus teléfonos inteligentes, y consideran la pérdida del teléfono más una molestia y no un riesgo. Si consideras al teléfono inteligente como un dispositivo de computación que siempre se encuentra conectado a una red y continuamente es trasladado de un lugar a otro, se destaca la diferencia entre portar información discreta y pasiva como la billetera, y portar un elemento activo e interactivo como un teléfono inteligente.

Un simple ejercicio nos puede ilustrar esto:

Vacía el contenido de tu bolso o billetera, y tome en cuenta los elementos sensibles que contienen. Normalmente encontrarás: - Fotos de las personas que amas (~5 fotos) - Tarjetas de identificación (licencia de conducir, tarjetas de membresía, documento de identidad, etc) - Seguros e información médica (~2 tarjetas) - Dinero (~5 billetes) - Tarjetas de Crédito/Débito (~3 tarjetas)

Ahora examina los contenidos de tu teléfono inteligente. Un usuario típico de teléfono inteligente podría encontrar más cantidad de información que la descrita anteriormente, y en algunos casos muchos más elementos sensibles y valiosos: - Fotos de las personas que amas (~100 fotos) - Aplicaciones de correo electrónico y sus contraseñas - Correos electrónicos (~500 correos) - Videos (~50 videos) - Aplicaciones de redes sociales y sus contraseñas - Aplicaciones de bancos en internet (con acceso a cuentas bancarias) - Documentos sensibles - Registros sensibles de comunicaciones - Conexión inmediata a tu información sensible

Entre más utilizas los teléfonos inteligentes, debes ser más consciente de los riesgos asociados a ellos y tomar las precauciones necesarias. Los teléfonos inteligentes son potentes amplificadores y distribuidores de tus datos personales. Están diseñados para proporcionar la mayor conectividad posible y acceder automáticamente a los servicios de redes sociales. Esto se debe a que tus datos personales son muy valiosos, y pueden ser agregados, buscados y vendidos.

En el ***Capítulo 5: Recuperar información perdida*** [249] conversamos sobre la importancia de respaldar datos. Esto aplica especialmente para teléfonos inteligentes. Sería un desastre si pierdes tu teléfono sin haber respaldado en un lugar seguro los datos más importantes (tales como tus contactos). Además de respaldar tus datos, asegúrate de conocer cómo recuperar los datos. Guarde una copia impresa de los pasos que debes seguir para que puedas hacerlo rápidamente en caso de emergencia.

En este capítulo iniciaremos con algunos elementos básicos de los teléfonos inteligentes – una descripción de varias plataformas y algunos procedimientos de configuración básicos para la seguridad de tu información y comunicación. Las otras secciones de este capítulo las dedicaremos a cubrir las precauciones específicas relacionadas con los usuarios comunes de teléfonos inteligentes. Secciones posteriores abordarán aspectos de seguridad sobre:

Plataformas, Configuración básica e Instalación

Plataformas y Sistemas Operativos

Al momento de escribir este capítulo, los teléfonos inteligentes de uso más común son el iPhone de Apple y Android de Google, seguidos por el Blackberry y teléfonos de Windows. La mayor diferencia entre el Android y los otros sistemas operativos, es que Android es un sistema, principalmente de Código Abierto (*FOSS* [250]), permitiendo que su sistema operativo sea auditado de forma independiente para verificar si protege apropiadamente la información y comunicación de los usuarios. También facilita el desarrollo de aplicaciones de seguridad para su plataforma. Muchos programadores conscientes de la seguridad desarrollan aplicaciones para Android pensando siempre en la seguridad del usuario. Algunas de estas aplicaciones las destacaremos más adelante en este capítulo.

Sin importar el tipo de teléfono inteligente que utilizas, es importante que seas consciente de algunos temas al usar un teléfono que se conecta a internet y que contiene características tales como *GPS* [251] o capacidad de red inalámbrica. En este capítulo nos enfocamos en dispositivos con la plataforma Android, ya que, como explicamos anteriormente, es más fácil asegurar datos y comunicaciones. Sin embargo, las guías de configuración básicas y algunas aplicaciones para dispositivos que no sean teléfonos Android se proporcionan también.

Los teléfonos Blackberry han sido presentados como dispositivos “seguros” para mensajería y correo electrónico. Esto porque los mensajes y correos electrónicos son dirigidos de forma segura por medio de los servidores de Blackberry, fuera del alcance de potenciales intrusos. Desafortunadamente, más y más gobiernos están demandando acceso a estas comunicaciones, citando la necesidad de protegerse contra el terrorismo y crimen organizado. La India, Emiratos Árabes

Unidos, Arabia Saudita, Indonesia y el Líbano son ejemplos de gobiernos que han analizado el uso de dispositivos Blackberry y han exigido el acceso a los datos del usuario en sus países.

Teléfonos móviles convencionales

Otra categoría de teléfonos móviles son llamados comúnmente 'móviles convencionales' (eje. Nokia 7705 Twist o Samsung Rogue). Recientemente, los móviles convencionales han incrementado sus funcionalidades para incluir algunas contenidas en los teléfonos inteligentes. Pero generalmentes, los sistemas operativos de los móviles convencionales son menos accesibles, y por lo tanto existen limitadas oportunidades para aplicaciones de seguridad o mejoras a las mismas. No abordamos específicamente los móviles convencionales, sin embargo muchas de las medidas expresadas en este capítulo también tienen sentido para los móviles convencionales.

Teléfonos inteligentes de marca y bloqueados

Los teléfonos inteligentes usualmente son vendidos con una marca o bloqueados. Un teléfono inteligente bloqueado significa que el dispositivo sólo puede ser operado con un único proveedor, y el dispositivo sólo funciona con su tarjeta SIM. Los proveedores de redes móviles usualmente le ponen marca a los teléfonos mediante la instalación de su propio “firmware” o software. También puede que los proveedores deshabiliten algunas funcionalidades o agregar otras. La marca es un medio para que las empresas aumenten sus ingresos mediante la canalización del uso de tu teléfono inteligente, a menudo también la recopilando datos acerca de cómo utilizas el teléfono o habilitando el acceso remoto a tu teléfono inteligente.

Por estas razones, recomendamos comprar teléfonos inteligentes desbloqueados, siempre que puedas. Un teléfono bloqueado incrementa los riesgos debido a que tus datos son canalizados a través de un sólo proveedor, centralizando así el flujo de tu información haciendo imposible cambiar las tarjetas SIM para difundir los datos a través de diferentes proveedores. Si tu teléfono está bloqueado, pregúntale a alguien de confianza cómo desbloquearlo.

Configuración General

Los teléfonos inteligentes tienen muchas opciones de configuración que controlan la seguridad del dispositivo. Es importante prestar atención sobre como se encuentra configurado tu teléfono inteligente. En las guías prácticas que se presentan más adelante, te alertaremos sobre algunas opciones de seguridad del teléfono inteligente que están disponibles pero no están activadas por defecto, así como aquellas opciones que se encuentran activadas por defecto y que vulneran tu teléfono.

Guía Práctica: Empezar con la *Guía de Configuración Básica de Android* [252]

Instalar y actualizar aplicaciones

La forma más común de instalar nuevo software en tu teléfono inteligente es usando el Appstore de iPhone o Google Play store, allí ingresas tu información de usuario, y descargas e instalas la aplicación que deseas. Al iniciar la sesión, estás asociando tu información de cuenta de usuario a la tienda virtual. Los dueños de la tienda virtual mantienen registros del historial de navegación del usuario y sus preferencias de aplicaciones.

Las aplicaciones que ofrecen las tiendas virtuales oficiales son, supuestamente, verificadas por los dueños de las tiendas (Google o Apple), pero en la realidad esto provee poca protección contra lo que puede hacer la aplicación una vez instalada en tu teléfono. Por ejemplo, algunas aplicaciones pueden copiar y enviar tu directorio de contactos luego de ser instaladas en tu teléfono. En el caso de los teléfonos Android, durante el proceso de instalación cada aplicación te solicita permiso sobre lo que puede o no hacer una vez en uso. Deberías prestar mucha atención a los tipos de permisos solicitados, y si estos permisos tienen sentido respecto a la funcionalidad de la aplicación que estás instalando. Por ejemplo, si estás considerando instalar una aplicación para “lectura de noticias” y te das cuenta que te solicita derechos para enviar tus contactos a través de una conexión móvil de datos a terceros, deberías buscar otras aplicaciones más acordes con accesos y derechos.

Las aplicaciones de Android también están disponibles fuera de los canales oficiales de Google. Sólo debes marcar la caja de *Fuentes desconocidos* que se encuentra en *Aplicaciones* para poder utilizar estos sitios web de descargas.

Son muy útiles estos sitios web alternativos si quieres minimizar tu contacto en línea con Google. Recomendamos **F-Droid** [253] ('Free Droid'), que sólo ofrece aplicaciones de *FOSS* [254]. En esta guía, F-Droid es el repositorio primordial de las aplicaciones que recomendamos, y sólo te referimos a Google Play si una aplicación no está disponible en F-Droid.

Si no deseas (o no puedes) conectarte a internet para acceder a las aplicaciones, puedes transferir aplicaciones al teléfono de otra persona enviando archivos *.apk* [255] (siglas del inglés para 'paquetes de aplicaciones para android') vía bluetooth. Como alternativa también puedes descargar el archivo .apk a la tarjeta Micro SD de tu dispositivo móvil o utilizar un cable usb para trasladarlo desde una computadora. Cuando hayas recibido el archivo, simplemente haz un pulso largo al archivo y estará listo para instalarse. (**Nota**: sea especialmente cuidadoso/a mientras usas bluetooth – leer más en ***Capítulo 10.2.4: Funciones más allá de la conversación y los mensajes*** [256]).

Comunicándote (Voz y Mensajes) vía Teléfono Inteligente

Conversaciones Seguras

Telefonía Básica

En el capítulo ***10.2.2 Funciones básicas, capacidad de rastreo y anonimato*** [257] conversamos sobre las diferentes medidas que deberías considerar para aminorar los riesgos de interceptación al utilizar los operadores de redes móviles para la comunicación de voz.

Utilizar la internet a través de tu teléfono inteligente sobre conexiones móviles de datos o WiFi puede ofrecer muchas opciones para comunicarte de forma segura con las personas, utilizando por ejemplo *VoIP* [258] e implementando medios para asegurar este canal de comunicación. Incluso, algunos teléfonos inteligentes pueden extender la seguridad a llamadas de teléfono móvil, más allá de VoIP (Ver **Redphone** abajo).

Aquí enumeramos algunas herramientas, con sus pros y contras:

Skype

La aplicación comercial VoIP más popular *Skype* [259] está disponible para todas las plataformas de teléfonos inteligentes y funciona si tu conexión inalámbrica es fiable. Es menos seguro en conexiones de data móvil.

En la ***Sección 3*** [260] del ***Capítulo 7: Mantener privada tu comunicación en Internet*** [260], conversamos sobre los riesgos al utilizar Skype, y porqué, si es posible, debemos evitar usuarlo. En resumen, Skype no es un software de Código Abierto lo que dificulta verificar de forma independiente sus niveles de seguridad. Adicionalmente, Skype es propiedad de Microsoft, el cual tiene el interés comercial de saber cuándo utilizas Skype y desde dónde. Así mismo, Skype podría permitirle a las agencias de la fuerza del orden acceso retrospectivo de todo tu historial de comunicaciones.

Otros VoIP

Utilizar VoIP generalmente es gratuito (o significativamente más barato que las llamadas móviles) y deja menos rastros de tus datos. Es más, una llamada segura con VoIP puede ser la forma más segura de comunicarse.

CSipSimple [261] es un poderoso cliente VoIP para teléfonos Android, que cuenta con excelente mantenimiento y contiene sencillas configuraciones de asistente para diferentes servicios VoIP.

Open Secure Telephony Network (OSTN) [262] y el servidor de Guardian project, **ostel.me** [263], actualmente ofrece uno de los medios más seguros para la comunicación de voz. Conocer y confiar en el proveedor que opera el servidor de tu comunicación VoIP es de vital importancia. Los que hospedan este servicio – **Guardian Project** [264] – son bien conocidos y respetados en la comunidad.

Al utilizar CSipSimple, nunca te comunicas directamente con la otra persona, en vez de ello todos tus datos se canalizan a través del servidor Ostel. Esto hace que sea mucho más difícil rastrear tus datos y averiguar con quién te estás hablando. Adicionalmente, Ostel no guarda ninguna información, excepto los datos de la cuenta que necesitas para iniciar la sesión. Todas tus conversaciones están cifradas; y tus meta datos (los cuales son usualmente muy difíciles de ocultar) son borrosas porque el tráfico pasa por el servidor ostel.me. Si descargas CSipSimple desde ostel.me, ya vendrá configurado para utilizarlo con ostel.me lo que lo hace aún más fácil de instalar y usar.

RedPhone [265] es una aplicación gratuita y Código Abierto que cifra datos de comunicación de voz enviados entre dos dispositivos que corren con esta misma aplicación. Es fácil de instalar y fácil de utilizar, ya que se integra a tu marcado normal y sistema de contactos. Sin embargo las personas con las que deseas comunicarte también necesitan instalar y utilizar RedPhone. Para facilitar el uso RedPhone utiliza su número de teléfono móvil como su identificador (como un nombre de usuario en otros servicios VoIP). Sin embargo, se vuelve más sencillo analizar el tráfico que produce y rastrearte de vuelta a través de tu número de teléfono móvil. RedPhone utiliza un servidor central como punto de centralización pone a RedPhone en una poderosa posición (por tener control sobre algunos esto datos).

Estamos desarrollando las Guías Prácticas para CSipSimple, Ostel.me y Redphone. Por el momento, puedes encontrar más información en los enlaces disponibles arriba.

Enviando Mensajes de forma Segura

Debes tomar precauciones a la hora de enviar SMS o al utilizar mensajería instantánea o chat en tu teléfono inteligente.

SMS

Como se describe en el ***Capítulo 10.2.3 Comunicaciones textuales – SMS / Mensajes de Texto*** [266], la comunicación SMS es insegura por defecto. Cualquier persona con acceso a una red de telecomunicación móvil puede interceptar fácilmente los mensajes, y esto es una acción cotidiana que se da en muchas situaciones. No se confíe enviando mensajes SMS inseguros en situaciones críticas. No existen ninguna forma de autenticar un mensaje SMS, por lo tanto es imposible saber si el contenido de dicho mensaje fue alterado durante su envío o si el emisor del mensaje realmente es la persona que dice ser.

Asegurando los SMS

TextSecure [267] es una herramienta de Código Abierto *FOSS* [254] para enviar y recibir SMS de forma segura en los teléfonos Android. Funciona tanto para mensajes cifrados y no cifrados, así que puedes utilizarla por defecto como una aplicación SMS. Para intercambiar mensajes cifrados esta herramienta debe estar instalado tanto por parte del emisor como del receptor del mensaje, por lo tanto deberás promover su uso constante entre las personas con las que te comunicas. TextSecure automáticamente detecta los mensajes cifrados recibidos desde otro usuario de TextSecure. También te permite cifrar mensajes a más de una persona. Los mensajes son firmados automáticamente haciendo casi imposible que los contenidos del mensaje sean alterados. En nuestras guía sobre TextSecure explicamos en detalle las características de esta herramienta y cómo utilizarla.

Guía Práctica: Empezar con la *Guía de TextSecure* [268]

Chat Seguro

La mensajería instantánea o chat en tu teléfono puede producir mucha información vulnerable a la interceptación. Estas conversaciones podrían ser usadas en tu contra por adversarios posteriormente. Deberías por lo tanto ser extremadamente cauteloso/a sobre lo que escribes en tu teléfono mientras envías mensajes instantáneos y al chatear.

Existen formas seguras para chatear y enviar mensajes instantáneos. La mejor forma es utilizar cifrado de extremo a extremo (doble vía), asegurando que la persona al otro extremo sea la persona con la que deseas comunicarte.

Recomendamos **Gibberbot** [269] por ser una aplicación segura para chatear en teléfonos Android. Gibberbot ofrece cifrado sencillo y fuerte para tus chats con el protocolo de mensajería *Off-the-Record* [270]. Este cifrado provee ambas autentificaciones, por un lado puedes verificar que chateas con la persona correcta, y por otro lado contiene seguridad independiente entre cada sesión, de esta forma si una sesión de chat cifrado se ve comprometida, otras sesiones pasadas o futuras se mantendrán seguras.

Gibberbot ha sido diseñado para funcionar en conjunto con Orbot, de esta forma tus mensajes de chat son canalizados a través de la red anónima *Tor* [142]. Esto hace que sea muy difícil de rastrear o incluso averiguar si sucedió alguna vez.

Guía Práctica: Empezar con *Gibberbot Guide* [271]

Para clientes de iPhones, el **ChatSecure** [272] provee las mismas características, sin embargo no es tan sencillo utilizarlo con la red de *Tor* [273].

Estamos desarrollando las Guías Prácticas para ChatSecure. Por el momento, puedes encontrar más información en homepage [272].

Independientemente de la aplicación que utilices, siempre considera desde cuál cuenta usarás el chat. Por ejemplo, cuando utilizas Google Talk, tus credenciales y tiempo de la sesión del chat serán conocidas por Google. Ponte de acuerdo con tus contactos para no dejar guardados los historiales de chat, especialmente si no están cifrados.

Guardando Información en tu Teléfono Inteligente

Los teléfonos inteligentes vienen con gran capacidad de almacenamiento de datos. Desafortunadamente, los datos guardados en tu dispositivo pueden ser fácilmente accesibles a terceras personas, ya sea de forma remota o con acceso físico al teléfono. Algunas precauciones básicas sobre cómo reducir el acceso indebido a esta información se explica en la ***Guía de Configuración Básica para Android*** [252]. Adicionalmente, puedes tomar medidas para cifrar información sensible en tu teléfono utilizando herramientas específicas.

Herramientas para cifrar datos

El **Android Privacy Guard (APG)** [274] permite cifrar archivos y correos electrónicos con OpenGPG. También puede ser usado para mantener tus archivos y documentos seguros en tu teléfono, así como cuando envías correos electrónicos.

Guía Práctica: Empezar con *APG Guide* [274]

El **Cryptonite** [275] es otra herramienta de Código Abierto *FOSS* [254] para cifrar archivos. Cryptonite tiene características más avanzadas para teléfonos Android especialmente preparados con firmware personalizado. Para más información, ver la sección ***Uso Avanzado de Teléfonos Inteligentes*** [276].

Guía Práctica: Empezar con *Cryptonite Guide* [277]

Manejo de Contraseñas Seguras

Puedes mantener todas tus contraseñas un solo lugar archivo cifrado de forma segura utilizando **Keepass**. Sólo deberás recordar una clave o contraseña maestra para acceder a todas las otras contraseñas. Con Keepass puedes usar contraseñas muy fuertes para cada una de tus cuentas, ya que Keepass las recordará para tí, además viene con un generador automático de contraseñas para crear contraseñas nuevas. Puedes sincronizar la base de datos de Keepass entre tu teléfono y tu computadora. Te recomendamos sincronizar sólo aquellas contraseñas que usas cotidianamente en

tu teléfono móvil. Puedes crear y separar en pequeñas bases de datos las contraseñas en la computadora, y posteriormente sincronizar una a tu teléfono móvil en lugar de copiar la base de datos entera de todas tus contraseñas. Como todas tus contraseñas estarán protegidas por una contraseña maestra, es de vital importancia que esta contraseña sea muy fuerte para proteger tu base de datos de Keepass. Ver ***Capítulo 3: Crear y mantener contraseñas seguras*** [129].

Guía Práctica: Empezar con la *Mini Guia de Keepass* [278]

Enviando Correos Electrónicos con Teléfonos Inteligentes

En esta sección abordaremos brevemente el uso de correo electrónico con teléfonos inteligentes. Te instamos a revisar las secciones ***Asegurar tu correo electrónico*** [279] y ***Consejos para responder ante una sospecha de vigilancia de correo electrónico*** [127] en el ***Capítulo 7: Mantener privada tu comunicación en Internet*** [280] en las que conversamos sobre la seguridad básica del correo electrónico.

En primera instancia, considere si realmente necesitas acceder a tu correo electrónico con tu teléfono inteligente. Asegurar una computadora y su contenido, generalmente es más sencillo que hacerlo con un dispositivo móvil como el teléfono inteligente. Un teléfono inteligente es más suceptible a robos, vigilancia e intrusiones.

Si es absolutamente necesario acceder a tu correo electrónico a través de tu teléfono inteligente, existen acciones que puedes implementar para aminorar los riesgos:

- No consideres tu teléfono inteligente como el principal medio para acceder a tu correo electrónico. Descargar (y eliminar) correos electrónicos de un servidor de correos y guardarlos sólo en tu teléfono inteligente no es recomendable. Puedes configurar tu aplicación de correo electrónico para usar únicamente las copias de tus correos.
- Si utilizas correo cifrado con tus contactos, considere la instalación del mismo en tu teléfono móvil también. El beneficio adicional es que los correos cifrados permanecerán secretos si el teléfono cae en las manos equivocadas.

Guardar tu llave privada de cifrado en tu teléfono móvil puede parecer un riesgo. Sin embargo, el beneficio de poder enviar y guardar tus correos electrónicos cifrados y seguros en el dispositivo móvil pesa más que el riesgo. Considera generar un par de llaves únicas de cifrado para móvil (usando **APG** [281]) en tu teléfono inteligente, de esta forma evitas copiar tu llave privada de tu computadora al dispositivo móvil. Nota que esto requiere preguntarle a las personas con las que te comunicas, que también deben cifren sus correos electrónicos utilizando la llave única de cifrado de móviles.

Guía Práctica: Empezar con la *Guía sobre K9 y APG* [282]

Capturando Multimedias con Teléfonos Inteligentes

Capturar fotos, videos o audios con tu teléfono inteligente puede ser un medio poderoso para documentar y compartir eventos importantes. Sin embargo, es importante ser cuidadoso/a y respetuoso/a de la privacidad y seguridad de las personas fotografiadas, filmadas o grabadas. Por ejemplo, si tomas fotos o filmas y grabas un evento importante, puede ser peligroso para tí o para los que aparecen en las grabaciones si tu teléfono cae en las manos equivocadas. En estos casos, estas sugerencias pueden ser de ayuda:

- Ten un mecanismo de seguridad para subir los archivos multimedia en un lugar protegido en internet, y elimínalos del teléfono inmediatamente (tan pronto le sea posible).
- Usa herramientas para difuminar rostros de las personas que aparecen en las imágenes o videos, o distorsiona las voces de los audio y grabaciones de video, y sólo guarde las copias distorsionadas y difuminadas en archivos multimedia en tu dispositivo móvil.
- Proteja o remueva la meta información relacionada con tiempo y lugares dentro que quedan registrados en los archivos multimedia.

El **Guardian Project** [264] ha creado una aplicación de Código Abierto *FOSS* [254] llamada **ObscuraCam** [283] que identifica los rostros en las fotos y los difumina. Por supuesto que puedes escoger el modo de difuminación y qué deseas difuminar. Obscuracam también elimina las fotos originales, y si tienes un servidor para subir los multimedia grabados, provee funciones fáciles para subirlos.

Guía Práctica: Empezar con la *Guía de Obscuracam* [284]

En este momento, la organización de derechos humanos **Witness** [285] está trabajando con el Guardian project en una solución para los tres puntos expuestos anteriormente.

Acceso a Internet Seguro con Teléfonos Inteligentes

Según se abordó en el ***Capítulo 7: Mantener privada tu comunicación en Internet*** [280] y en el ***Capítulo 8: Mantenerse***

en el anonimato y evadir la censura en Internet [143], acceder a contenidos en Internet, o publicar fotos y videos, dejan huellas y rastros de quién eres y dónde estás y qué estás haciendo. Esto puede ponerte en riesgo. Utilizar tu teléfono inteligente para comunicarte con la internet aumenta considerablemente estos riesgos.

Acceso mediante WiFi o Data Móvil

Los teléfonos móviles te permiten controlar cómo accedes a Internet: vía conexión inalámbrica desde un punto de acceso (como un internet café o cyber), o vía conexión de data móvil, tales como GPRS, EDGE, o UMTS que ofrece tu proveedor de red móvil.

Utilizar una conexión WiFi reduce los rastros o huellas de los datos que estás dejando en tu proveedor de servicios de telefonía móvil (ya que no estás conectado/a con tu suscripción de teléfono móvil). A pesar de ello, algunas veces la conexión de data móvil es la única forma de estar en línea. Desafortunadamente, los protocolos de la conexión de data móvil (como EDGE o UMTS) no tienen protocolos abiertos. Desarrolladores independientes e ingenieros de seguridad no pueden examinar estos protocolos para ver cómo están siendo implementados por operadores de data móvil.

En algunos países los proveedores de servicios móviles operan bajo diferentes legislaciones que los proveedores de servicios de internet, lo que puede resultar en una mayor vigilancia por parte de gobiernos y responsables del soporte.

Independientemente del camino que tomes para tus comunicaciones digitales con teléfonos inteligentes, puedes reducir los riesgos de exponer datos mediante el uso de herramientas para el cifrado y anonimato.

Anonimizar

Para acceder a contenido en línea de forma anónima, puedes usar la aplicación para Android llamada **Orbot** [286]. Orbot canaliza tu comunicación en internet mediante la red anónima de Tor.

Guía Práctica: Empezar con la *Guía de Orbot* [287]

Otra aplicación llamada Orweb, tiene la característica de ser un navegador web con potentes características de privacidad utilizando proxies que no guardan el historial de la navegación local. Juntos Orbot y Orweb eluden los filtros y cortafuegos en la web, y ofrecen navegación anónima.

Guía Práctica: Empezar con la *Guía de Orweb* [288]

Proxies

La versión móvil del navegador *Firefox* [289] – **Firefox mobile** [290] puede equiparse con complementos proxy que dirigirán tu tráfico a un servidor proxy. Por lo tanto, tu tráfico irá al sitio que estás solicitando. Esto es poderoso en casos de censura, pero puede que revele tus solicitudes si tu conexión desde tu cliente al proxy no está cifrada. Recomendamos el complemento llamado **Proxy Mobile** [291] (también de el **Guardian Project** [292], el cual hace que el proxy con Firefox sea sencillo. Así mismo, es la única forma de canalizar la comunicación móvil de Firefox a Orbot y utilizar la red *Tor* [273].

Seguridad Avanzada para Teléfonos Inteligentes

Obtén acceso completo a tu teléfono inteligente

La mayoría de los teléfonos inteligentes son capaces de hacer más que lo que ofrece el sistema operativo instalado en ellos, del software manufacturado (firmware) o de los programas del operador móvil. Al contrario, algunas funcionalidades están "encerradas" por lo que el usuario no es capaz de controlar o alterar estas funciones, y están fuera de alcance. En la mayoría de casos, esas funcionalidades son innecesarias para los usuarios de teléfonos inteligentes. Sin embargo, existen algunas aplicaciones y funcionalidades que pueden aumentar la seguridad de datos y comunicaciones en el teléfono inteligente. También existen otras funciones existentes que se pueden remover para evitar riesgos a la seguridad.

Por esto, y por otras razones, algunos usuarios de teléfonos inteligentes prefieren manipular los diversos programas y software ya instalados en los teléfonos inteligentes con el fin de obtener privilegios que les permite instalar funciones mejoradas, o remover y/o reducir otras.

El proceso de superar los límites impuestos por el operador móvil, o manufactureros de los sistemas operativos en un teléfono inteligente se llaman “rooting” (en el caso de dispositivos de Android), o “jailbreaking” (en el caso de dispositivos iOS como iPhone o iPad). Normalmente, el éxito del “rooting” o “jailbreaking” tiene como resultado obtener todos los privilegios necesarios para instalar o utilizar aplicaciones adicionales, realizar modificaciones a configuraciones bloqueadas, y control total sobre los datos guardados y la memoria del teléfono inteligente.

ADVERTENCIA: El “rooting” o “jailbreaking” no es un proceso reversible, y requiere de experiencia en la instalación y configuración de software. Considere lo siguiente:

- Existe el riesgo de que tu teléfono inteligente quede permanentemente inoperable, o “bricking it” (eje convertirlo en un ladrillo).
- La garantía del manufacturero u operador móvil puede quedar sin efecto o anulada.
- En algunos lugares este proceso puede ser considerado ilegal.

Pero si eres cuidadoso/a, un dispositivo “rooted” puede ser una forma sencilla de obtener mayor control sobre los teléfonos inteligentes hacerlo mucho más seguro.

Firmware Alternativo

Firmware se refiere a programas que están estrechamente relacionados a un dispositivo en particular. Están en cooperación con el sistema operativo del dispositivo y son responsables de la operación básica del hardware de tu teléfono inteligente, tales como el micrófono, parlantes, cámara, pantalla táctil, memoria, llaves, antenas, etc.

Si tienes un dispositivo Android, puedes considerar instalarle un firmware alternativo para mejorar aún más tu control sobre el teléfono. Nota que para instalar firmware alternativo implementa el proceso de “rooting” a tu teléfono.

Un ejemplo de un firmware alternativo para un teléfono Android es **Cyanogenmod** [293], el cual te permite desinstalar aplicaciones al nivel del sistema de tu teléfono (eje, aquellas aplicaciones instaladas por el manufacturero del teléfono o tu operador de red móvil). Al hacerlo, puedes reducir la cantidad de formas en las que tu dispositivo es monitoreado, como cuando la información es enviada a tu proveedor de servicios sin tu conocimiento.

Adicionalmente, Cyanogenmod navega por defecto con una aplicación OpenVPN (RPV por sus siglas en español), que en caso contrario sería tedioso instalar. RPV (Red Privada Virtual, siglas en inglés) es una de las formas de asegurar el proxy de tu comunicación en internet (ver abajo).

Cyanogenmod también ofrece un modo de navegación Incógnito en el cual el historial de tus comunicaciones no es registrada en tu teléfono inteligente.

Cyanogenmod viene con muchas otras características. Sin embargo, no es compatible con todos los dispositivos de Android, así que antes de continuar revisa la lista de dispositivos compatibles [294].

Cifrar volúmenes completos

Si tu teléfono ha sido “rooted” quizá quieras cifrar todo el espacio de almacenamiento de datos, o bien crear un volumen en el teléfono inteligente para proteger alguna información en el teléfono.

Luks Manager [295] le permite cifrar volúmenes con alta seguridad y de forma instantánea mediante una interfaz amigable. Es altamente recomendable que instale esta herramienta antes de empezar a guardar datos en tu dispositivo Android y utilizar los Volúmenes Cifrados que provee el Luks Manager para almacenar tus datos.

El proyecto Whisper Systems está preparando un aplicación llamada **WhisperCore** [296] que te permitirá un cifrado total de tu dispositivo Android.

Red Privada Virtual (RPV)

Una RPV ofrece un túnel cifrado a través de la internet entre tu dispositivo y un servidor RPV. Esto se llama un túnel porque a diferencia de otros tráficos cifrados, como https, esconde todos los servicios, protocolos y contenidos. Una conexión RPV se configura una sola vez, y termina solo cuando tu lo decidas.

Ten en cuenta que como todo tu tráfico viaja a través de un servidor proxy o RPV, un intermediario sólo necesitará acceso al proxy para analizar tus actividades. Por lo tanto, es sumamente importante que escojas cuidadosamente entre los servicios de proxy y de RPV. También es recomendable utilizar diferentes proxys y/o RPV, ya que al distribuir en diferentes canales tus datos se reduce el impacto de un servicio en peligro.

Recomendamos el uso del servidor **RiseUp VPN** [297]. Puedes utilizar RiseUp VPN en un dispositivo Android después de instalar Cyanogenmod (ver arriba). Además es muy fácil de configurar la conexión del RiseUp VPN a un iPhone – para más información leer aquí [298].

Glosario

Algunos de los términos técnicos que encontrarás, a medida que leas estos capítulos, se define a continuación:

- ***Amenaza física*** – En este contexto, cualquier amenaza a tu información sensible que sea el resultado de la acción de otras personas que tengan acceso físico directo al hardware de tu computadora o cuyo origen sea otro riesgo físico tal como una rotura, accidente o desastre natural.
- ***Archivo de paginación o intercambio*** – Archivo en tu computadora en el cual se guarda información, parte de la cual puede ser sensible, ocasionalmente con el fin de mejorar su rendimiento.
- ***Arrancado*** – Acción de iniciar una computadora.
- ***Avast*** – Herramienta antivirus de software gratuito.
- ***Base de datos de contraseñas seguras*** – Herramienta que puede cifrar y almacenar tus contraseñas utilizando una única contraseña maestra.

- ***Cable de seguridad*** – Cable de cierre que puede utilizarse para asegurar, a una pared o un escritorio, una computadora portátil u otros equipos, entre ellos discos duros externos y algunas computadoras de escritorio. Ello con el fin de impedir que sean físicamente removidos del lugar.

- ***Capa de Conexión Segura (Secure Sockets Layer (SSL))*** – Tecnología que te permite mantener una conexión segura, *cifrada* entre tu computadora y algunos de los sitios web y los servicios de Internet que visitas. Cuando estas conectado a un sitio web a través de una capa de conexión segura (SSL), la dirección del sitio web empezará con ***HTTPS*** en vez de ***HTTP***.

- ***CCleaner*** – Herramienta de software libre que elimina los archivos temporales y los potencialmente sensibles rastros dejados en tu disco duro por programas que utilizaste recientemente y por el mismo sistema operativo Windows.

- ***Certificado de seguridad*** – Forma de garantizar que los sitios web y otros servicios de Internet, utilizando cifrado, son realmente quienes dicen ser. Sin embargo, con el fin de que tu navegador acepte un *certificado de seguridad* como valido, el servicio debe pagar por una *firma digital* de una organización confiable. Debido a que ello es oneroso algunos operadores de servicios son reticentes o incapaces de gastar en este. Sin embargo, de manera ocasional verás un error de *certificado de seguridad* incluso cuando visitas un servicio válido.

- ***Cifrado*** – Forma ingeniosa de utilizar las matemáticas para *cifrar*, o mezclar, información de modo que solo pueda ser *descifrada* y leída por quien tenga cierta información, tal como una contraseña o una *llave de cifrado*.

- ***Clam Win*** – Programa antivirus de software libre y de código abierto para Windows.

- ***Cobian Backup*** – Herramienta de respaldo de software libre y de código abierto. La última versión del Cobian es de software gratuito pero de código cerrado, sin embargo, las versiones anteriores fueron lanzadas como software gratuito y de código abierto.

- ***Código fuente*** – Código subyacente escrito por los programadores de computadoras que permite la creación de software. El código fuente para una herramienta dada revelará como funciona y si esta puede ser insegura o maliciosa.

- ***Código mnemotécnico*** – Un sistema simple que puede ayudarte a recordar contraseñas complejas.

- ***Comodo Firewall*** – Herramienta cortafuegos de software libre.

- **Cookie** – Pequeño archivo, que almacena tu navegador en tu computadora. Este puede utilizarse para almacenar información de, o para identificarte, en un sitio web particular.

- ***Corriente Eléctrica Ininterrumpida (UPS)*** – Equipo que permite a tus equipos de computación críticos que continúen operando, o que se apaguen paulatinamente ante la ocurrencia de una breve pérdida de energía.

- ***Cortafuegos (firewall)*** – Herramienta que protege a tu computadora de conexiones no confiables desde o hacia redes locales y la Internet.

- ***Dirección de Protocolo de Internet (dirección IP)*** – Identificador único asignado a tu computadora cuando se conecta a Internet.

- ***Eliminación Permanente*** – Proceso de borrado de información de manera segura y permanente.

- ***Enigmail*** – Complemento del programa de correo electrónico Thunderbird que le permite a este enviar y recibir correos electrónicos cifrados y firmados digitalmente.

- ***Enrutador (router)*** – Equipo de red a través del cual las computadoras se conectan a sus redes locales y por medio del cual varias redes locales acceden a Internet. *Interruptores (switches), pasarelas (gateways) y concentradores (hubs)* realizan tareas similares, del mismo modo que los puntos de acceso inalámbricos para computadoras que están apropiadamente equipadas para utilizarlos.

- ***Eraser*** – Herramienta que elimina información, de tu computadora o de tu dispositivo removible de almacenamiento, de manera segura y permanente.

- ***Esteganografía*** – Cualquier método de disfrazar información sensible de modo que aparezca ser algo distinto. Ello se hace con el fin de evitar atraer la atención hacia esta.

- ***Evasión*** – Acto de evadir los filtros de Internet para acceder a los sitios web y otros servicios de Internet bloqueados.

- ***Firefox*** – Popular navegador web de software libre y de código abierto que es una alternativa al Internet Explorer de Microsoft.

- ***Firma Digital*** – Forma de utilizar el cifrado para probar que un archivo o mensaje particular fue realmente enviado por la persona que afirma haberlo enviado.

- ***Fuera de Registro (OTR)*** – Complemento de cifrado del programa de mensajería instantánea *Pidgin*.

- ***GNU/Linux*** – Sistema operativo de software libre y código abierto que es una alternativa a Windows de Microsoft.
- ***HTTPS*** – Cuando estas conectado a un sitio web a través de una Capa de Conexión Segura (Secure Socket Layer (SSL)), la dirección del sitio web empezará con HTTPS en vez de HTTP.
- ***KeePass*** – Software libre de base de datos de contraseñas seguras
- ***Lista negra*** – Lista de sitios web y otros servicios de Internet bloqueados que no puede ser accedidos debido a una política restrictiva de filtrado.
- ***Lista blanca*** – Lista de sitios web o de servicios de Internet a los cuales cierta forma de acceso esta permitido, mientras que otros sitios son automáticamente bloqueados.
- ***LiveCD*** - Un CD que permite a tu computadora ejecutar un sistema operativo diferente en forma temporal.
- ***Nombre de dominio*** – La dirección, en palabras, de un sitio web o de un servicio de Internet; por ejemplo: security.ngoinabox.org
- ***NoScript*** – Complemento de seguridad para el navegador Firefox que te protege de programas maliciosos que podrían presentarse en páginas web desconocidas.
- ***Peacefire*** – Los suscriptores a este servicio gratuito reciben correos electrónicos periódicos que contienen una lista actualizada de proxies de evasión, los cuales pueden ser utilizados para eludir la censura en Internet.
- ***Pidgin*** – Herramienta de mensajería instantánea de software libre y de código abierto que se apoya en un complemento llamado *Fuera de Registro (OTR)*.
- ***Pirata informático (hacker)*** – En este contexto, un criminal informático malicioso quien puede intentar acceder a tu información sensible o tomar control de tu computadora de manera remota.
- ***Política de seguridad*** – Documento escrito que describe cómo tu organización puede protegerse de mejor manera de distintas amenazas, esta incluye una lista de pasos a seguir en caso ocurran ciertos eventos vinculados a la seguridad.
- ***Proveedor de Servicio de Internet (ISP)*** – La compañía u organización que provee tu conexión inicial a la Internet. Los gobiernos de muchos países ejercen control sobre la Internet, utilizando medios tales como el filtrado y la vigilancia, a través de los proveedores de servicios de Internet que operan en dichos países.
- ***Proxy*** – Servicio intermediario a través del cual puedes conducir algunas o todas tus comunicaciones por Internet y que puede ser utilizado para evadir la censura en Internet. Un proxy puede ser público, o podrías necesitar un nombre de usuario y una contraseña para conectarte a este. Solamente algunos proxies son seguros, lo que significa que utilizan cifrado para proteger la privacidad de la información que pasa entre tu computadora y los servicios de Internet a los cuales te conectas a través del proxy.
- ***Quemador de CD*** – Unidad CD-ROM de una computadora que puede escribir datos en CDs en blanco. Los *Quemadores de DVD* pueden hacer lo mismo con DVDs in blanco. Las *unidades de CD-RW* y *de DVD-RW* pueden borrar y reescribir información más de una vez en el mismo CD o DVD que cuente con estas características.
- ***Registrador de teclas (keylogger)*** – Tipo de software espía que registra que teclas has pulsado en el teclado de tu computadora y envía esta información a un tercero. Los registradores de teclas (keyloggers) son utilizados frecuentemente para robar correos electrónicos y otras contraseñas.
- ***Riseup*** – Servicio de correo electrónico administrado por y para activistas. A este servicio se puede acceder de manera segura a través de un servidor web de correo o utilizando un cliente de correo electrónico como el *Mozilla Thunderbird*.
- ***Servidor*** – Computadora que se mantiene encendida y conectada a la Internet con el fin de proporcionar algún servicio, como puede ser el alojamiento de una página web o el envío y recepción de correo electrónico a otras computadoras.
- ***Sistema Básico de Entrada/Salida (BIOS)*** – El primer y más profundo nivel de software en una computadora. El BIOS te permite fijar muchas opciones avanzadas vinculadas al hardware de la computadora, entre ellas la contraseña de encendido.
- ***Skype*** – Herramienta de software libre de voz sobre protocolo de Internet (VoIP) que te permite hablar gratuitamente con otros usuarios de Skype y hacer llamadas telefónicas pagando una tarifa. La compañía que respalda el Skype afirma que las conversaciones con otros usuarios de Skype son cifradas. Debido a que es una herramienta de código cerrado, no hay manera de verificar esta alegación, pero muchas personas creen que es cierta. Skype también ofrece el servicio de mensajería instantánea.
- ***Software gratuito (freeware)*** – Incluye software sin costo pero que está sujeto a restricciones legales o técnicas que le impiden al usuario acceder al código fuente utilizado para crearlo.
- ***Software Libre y de Código Abierto (FOSS)*** – Esta familia de software está disponible gratuitamente y no tiene restricciones legales que impidan a un usuario probarlo, compartirlo o modificarlo.

- ***Software malicioso (malware)*** – Término general para referirse a cualquier software malicioso, entre ellos *virus, software espía (spyware), troyanos,* y otras amenazas similares.

- ***Software propietario*** – Es el opuesto al software libre y de código abierto (FOSS). Estas aplicaciones son normalmente comerciales, pero también pueden ser *software libre* con requisitos de licencia restrictivos.

- ***Spybot*** – Herramienta de software libre que combate el software malicioso (malware), por ello escanea, elimina y ayuda a proteger tu computadora de cualquier software espía (spyware).

- ***Tarjeta SIM*** – Tarjeta pequeña y desmontable que puede ser insertada en un teléfono móvil con el fin de proporcionar servicio con una compañía de telefonía móvil en particular. Las tarjetas SIM también pueden almacenar números telefónicos y mensajes de texto.

- ***Thunderbird*** – Programa de correo electrónico de software libre y de código abierto con varias características de seguridad, entre ellas la admisión del complemento de cifrado *Enigmail*.

- ***Tor*** – Herramienta de anonimato que te permite evadir la censura en Internet y ocultar las páginas web y servicios de Internet que visitas de cualquiera que pudiera estar vigilando tu conexión a Internet. Al mismo tiempo esta herramienta oculta tu ubicación a aquellos sitios web a los que ingresas.

- ***TrueCrypt*** – Herramienta de cifrado de archivos de software libre y código abierto que te permite almacenar información sensible de manera segura.

- ***Undelete Plus*** – Herramienta de software libre que a veces puede restituir la información que pudieras haber borrado de manera accidental.
- ***VauletSuite 2 Go*** - Programa de software gratuito para cifrado de correo electrónico.

- ***Voz sobre Protocolo de Internet (VoIP)*** – Tecnología que te permite utilizar Internet para comunicaciones por voz con otros usuarios de *Voz sobre Protocolo de Internet* y teléfonos.

- ***Your-Freedom*** – Herramienta de evasión de software libre que te permite evadir filtros en la Internet por medio de una conexión a un proxy privado. Si Your-Freedom esta configurado adecuadamente, tu conexión a estos proxies será cifrada con el fin de proteger la privacidad de tus comunicaciones.

Enlaces:
[1] https://securityinabox.org/glossary#Hacker
[2] https://securityinabox.org/glossary#Malware
[3] https://securityinabox.org/glossary#Avast
[4] https://securityinabox.org/glossary#Spybot
[5] https://securityinabox.org/glossary#Comodo_Firewall
[6] https://securityinabox.org/glossary#GNU_Linux
[7] https://securityinabox.org/glossary#Freeware
[8] https://securityinabox.org/glossary#FOSS
[9] https://securityinabox.org/es/glossary#Freeware
[10] https://securityinabox.org/es/glossary#Avast
[11] https://securityinabox.org/es/avast_principal
[12] https://securityinabox.org/es/glossary#Clam_Win
[13] https://securityinabox.org/es/glossary#FOSS
[14] https://securityinabox.org/es/avast_utilizar#Seccion_3.2.1
[15] https://securityinabox.org/spybot_principal
[16] https://securityinabox.org/glossary#Firefox
[17] https://securityinabox.org/glossary#NoScript
[18] https://securityinabox.org/firefox_noscript
[19] https://securityinabox.org/firefox_principal
[20] https://securityinabox.org/glossary#Firewall
[21] https://securityinabox.org/es/comodo_principal
[22] https://securityinabox.org/chapter_1_5
[23] https://securityinabox.org/glossary#Router
[24] https://securityinabox.org/glossary#Software_propietario
[25] https://securityinabox.org/glossary#Codigo_fuente
[26] https://securityinabox.org/glossary#Thunderbird
[27] https://securityinabox.org/glossary#LiveCD
[28] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_9.html
[29] http://www.frontlinedefenders.org/manual/en/esecman/appendix_c.html
[30] http://www.frontlinedefenders.org/manual/en/esecman/
[31] http://www.virusbtn.com/
[32] https://security.berkeley.edu/MinStds/Determining-Un-Services-Windows.html
[33] http://www.marksanborn.net/howto/turn-off-unnecessary-windows-services
[34] http://www.tacticaltech.org/
[35] http://www.ngoinabox.org/
[36] http://www.askvg.com/download-free-bootable-rescue-cds-from-kaspersky-bitdefender-avira-f-secure-and-others/
[37] http://www.selectrealsecurity.com/malware-removal-guide/
[38] http://www.frontlinedefenders.org/manual/en/esecman
[39] http://www.virusbtn.com
[40] http://www.tacticaltech.org
[41] https://securityinabox.org/glossary#Politica_seguridad

[42] https://securityinabox.org/glossary#Amenaza_fisica
[43] https://securityinabox.org/glossary#Skype
[44] https://securityinabox.org/glossary#Servidor
[45] https://securityinabox.org/chapter-3
[46] https://securityinabox.org/glossary#BIOS
[47] https://securityinabox.org/glossary#Arrancado
[48] https://securityinabox.org/glossary#Cifrado
[49] https://securityinabox.org/chapter-4
[50] https://securityinabox.org/glossary#Cable_seguridad
[51] https://securityinabox.org/glossary#UPS
[52] https://securityinabox.org/chapter-5
[53] https://securityinabox.org/chapter_2_5
[54] http://www.frontlinedefenders.org/manual/en/esecman/chapter1_2.html
[55] http://www.frontlinedefenders.org/manual/en/esecman/chapter1_3.html
[56] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_1.html#2_1c
[57] http://www.frontlinedefenders.org/manual/en/esecman/chapter4.html
[58] http://www.frontlinedefenders.org/manuals/protection
[59] http://www.frontlinedefenders.org/es/node/15204
[60] http://www.frontlinedefenders.org/manuals
[61] https://securityinabox.org/glossary#BD_contrasena_segura
[62] https://securityinabox.org/glossary#KeePass
[63] https://securityinabox.org/chapter_3_2
[64] https://securityinabox.org/glossary#Dispositivos_nemotecnicos
[65] https://securityinabox.org/glossary#BD_contrasenas_seguras
[66] https://securityinabox.org/keepass_principal
[67] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_2.html
[68] http://www.frontlinedefenders.org/manual/en/esecman/appendix_d.html
[69] http://en.wikipedia.org/wiki/Password
[70] http://en.wikipedia.org/wiki/Password_strength
[71] http://en.wikipedia.org/wiki/Password_cracking
[72] http://www.en.wikipedia.org/wiki/Password
[73] http://www.en.wikipedia.org/wiki/Password_strength
[74] http://www.en.wikipedia.org/wiki/Password_cracking
[75] https://securityinabox.org/chapter-1
[76] https://securityinabox.org/chapter-2
[77] https://securityinabox.org/glossary#TrueCrypt
[78] https://securityinabox.org/es/truecrypt_principal
[79] https://securityinabox.org/chapter_4_2
[80] https://securityinabox.org/chapter-6
[81] https://securityinabox.org/truecrypt_principal
[82] https://securityinabox.org/glossary#Esteganografia
[83] https://securityinabox.org/chapter_4_3
[84] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_4.html
[85] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_8.html
[86] http://www.frontlinedefenders.org/manual/en/esecman/chapter4_2.html
[87] http://www.truecrypt.org/faq.php
[88] https://securityinabox.org/glossary#Cobian_Backup
[89] https://securityinabox.org/glossary#Undelete_Plus
[90] https://securityinabox.org/thunderbird_principal
[91] https://securityinabox.org/glossary#Quemador_CD
[92] https://securityinabox.org/chapter_5_5
[93] https://securityinabox.org/cobian_principal
[94] https://securityinabox.org/es/recuva_principal
[95] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_3.html
[96] https://www.wuala.com/
[97] https://spideroak.com/
[98] https://drive.google.com/start/
[99] https://tahoe-lafs.org/trac/tahoe-lafs/
[100] http://en.wikipedia.org/wiki/Data_recovery
[101] https://www.wuala.com
[102] https://spideroak.com
[103] https://drive.google.com/start
[104] https://tahoe-lafs.org/trac/tahoe-lafs
[105] http://www.en.wikipedia.org/wiki/Data_recovery
[106] https://securityinabox.org/glossary#Eraser
[107] https://securityinabox.org/glossary#Eliminacion
[108] https://securityinabox.org/glossary#CCleaner
[109] https://securityinabox.org/glossary#Archivo_intercambio
[110] https://securityinabox.org/eraser_principal
[111] https://securityinabox.org/glossary#Cookie
[112] https://securityinabox.org/ccleaner_principal
[113] https://securityinabox.org/es/firefox_principal
[114] http://support.mozilla.com/en-US/kb/Clearing+Private+Data
[115] http://www.ccleaner.com/help/faq
[116] http://www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/
[117] http://www.en.wikipedia.org/wiki/Gutmann_method
[118] http://www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann
[119] https://securityinabox.org/glossary#VoIP
[120] https://securityinabox.org/glossary#RiseUp
[121] https://securityinabox.org/glossary#OTR
[122] https://securityinabox.org/glossary#Pidgin
[123] https://securityinabox.org/glossary#Enigmail
[124] https://securityinabox.org/glossary#Keylogger
[125] https://securityinabox.org/es/chapter_7_4
[126] https://securityinabox.org/es/chapter_7_4#Cifrarautenticarmensajes
[127] https://securityinabox.org/es/chapter_7_2
[128] https://securityinabox.org/es/chapter-1

[129] https://securityinabox.org/es/chapter-3
[130] https://securityinabox.org/es/glossary#ISP
[131] https://securityinabox.org/es/glossary#Cifrado
[132] https://securityinabox.org/es/glossary#SSL
[133] https://securityinabox.org/es/glossary#Certificado_seguridad
[134] https://securityinabox.org/es/glossary#Firefox
[135] https://securityinabox.org/es/glossary#IP
[136] https://securityinabox.org/es/chapter_7_5
[137] https://securityinabox.org/es/glossary#Riseup
[138] https://mail.riseup.net
[139] https://securityinabox.org/es/riseup_principal
[140] https://securityinabox.org/es/glossary#Thunderbird
[141] https://securityinabox.org/es/thunderbird_principal
[142] https://securityinabox.org/es/glossary#Tor
[143] https://securityinabox.org/es/chapter-8
[144] https://securityinabox.org/es/glossary#Evasion
[145] https://securityinabox.org/es/chapter-6
[146] https://securityinabox.org/es/ccleaner_principal
[147] https://securityinabox.org/chapter-8
[148] https://securityinabox.org/es/glossary#VoIP
[149] https://securityinabox.org/es/glossary#Pidgin
[150] https://securityinabox.org/es/glossary#OTR
[151] https://securityinabox.org/es/pidgin_principal
[152] https://securityinabox.org/es/glossary#Skype
[153] http://www.jitsi.com/pc
[154] http://www.google.com/talk
[155] http://www.voice.yahoo.com
[156] http://www.download.live.com/?sku=messenger
[157] http://www.skype.com
[158] https://securityinabox.org/es/gpg4usb_portatil
[159] https://securityinabox.org/es/glossary#Enigmail
[160] https://securityinabox.org/en/glossary#VaultletSuite
[161] https://securityinabox.org/es/vaultletsuite_principal
[162] https://securityinabox.org/es/glossary#Firma_digital
[163] https://securityinabox.org/es/thunderbird_usarenigmail
[164] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_5.html#2_5b
[165] https://securityinabox.org/riseup_principal
[166] http://help.riseup.net/mail/mail-clients/
[167] http://mail.google.com/support/bin/topic.py?topic=12805
[168] http://email.about.com/od/mozillathunderbirdtips/qt/et_gmail_addr.htm
[169] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_7.html#2_7c
[170] http://mail.google.com/mail/help/intl/en/privacy.html
[171] http://news.cnet.com/8301-13578_3-9962106-38.html
[172] http://www.gizmo5.com/pc
[173] https://mail.google.com/mail/help/intl/en/privacy.html
[174] http://www.news.cnet.com/8301-13578_3-9962106-38.html
[175] http://help.riseup.net/mail/mail-clients
[176] https://mail.google.com/support/bin/topic.py?topic=12805
[177] http://www.email.about.com/od/mozillathunderbirdtips/qt/et_gmail_addr.htm
[178] https://securityinabox.org/glossary#IP
[179] https://securityinabox.org/glossary#Nombre_dominio
[180] https://securityinabox.org/glossary#Evasion
[181] https://securityinabox.org/glossary#Proxy
[182] https://securityinabox.org/glossary#ISP
[183] http://opennet.net/
[184] http://www.rsf.org/
[185] https://securityinabox.org/glossary#isp
[186] https://securityinabox.org/glossary#Lista_negra
[187] https://securityinabox.org/glossary#lista_negra
[188] http://www.blogger.com
[189] https://securityinabox.org/glossary#Tor
[190] https://securityinabox.org/glossary#HTTPS
[191] https://securityinabox.org/tor_principal
[192] https://securityinabox.org/glossary#Psiphon
[193] https://securityinabox.org/glossary#Peacefire
[194] https://securityinabox.org/glossary#SSL
[195] https://sesawe.net/Using-psiphon-2.html
[196] https://securityinabox.org/chapter_8_3#Redesanonimas
[197] https://securityinabox.org/chapter_8_5
[198] https://sesawe.net/Anchor-Free-Hotspot-Shield.html
[199] https://securityinabox.org/glossary#Your-Freedom
[200] http://www.your-freedom.net/index.php?id=3
[201] http://www.your-freedom.net/index.php?id=170&L=0
[202] http://your-freedom.net/
[203] http://sesawe.net/Using-Your-Freedom.html
[204] mailto:get@psiphon3.com
[205] http://www.psiphon.ca/
[206] http://www.peacefire.org/
[207] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_5.html#2_5d
[208] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_6.html
[209] http://en.flossmanuals.net/CircumventionTools
[210] http://sesawe.net/
[211] http://en.cship.org/wiki/Main_Page
[212] http://www.civisec.org/sites/securitybkp.ngoinabox.org/themes/civisec/guides/everyone%27s-guide-english.pdf
[213] http://www.rsf.org/rubrique.php3?id_rubrique=542
[214] http://advocacy.globalvoicesonline.org/projects/guide/
[215] http://www.opennet.net

[216] http://www.rsf.org
[217] http://www.psiphon.ca
[218] http://www.hotspotshield.com
[219] http://www.your-freedom.net/index.php?id=170
[220] http://www.your-freedom.net
[221] https://sesawe.net/Using-Your-Freedom.html
[222] http://www.peacefire.org
[223] http://www.flossmanuals.net/CircumventionTools
[224] https://sesawe.net/
[225] http://www.en.cship.org/wiki/Main_Page
[226] http://advocacy.globalvoicesonline.org/tools/guide
[227] https://securityinabox.org/en/chapter-3
[228] https://www.eff.org/wp/locational-privacy
[229] http://www.facebook.com/terms.php
[230] http://www.facebook.com/privacy/
[231] http://www.facebook.com/editapps.php
[232] http://www.facebook.com/privacy/explanation.php
[233] http://twitter.com/terms
[234] http://joindiaspora.com
[235] http://we.riseup.net
[236] https://securityinabox.org/en/node/1777
[237] https://securityinabox.org/en/node/1778
[238] https://securityinabox.org/en/node/1779
[239] https://securityinabox.org/en/node/1780
[240] http://wiki.mobiles.tacticaltech.org/index.php/Main_Page
[241] http://wiki.mobiles.tacticaltech.org/index.php/Security
[242] http://www.activistsecurity.org/
[243] http://www.freebeagles.org/articles/mobile_phones.html
[244] http://mobileactive.org/mobilesecurity-citizenjournalism
[245] http://sw.nokia.com/id/5274b81c-12d0-43bb-8d89-26f6a1ae111f/A_Brief_Introduction_to_Secure_SMS_Messaging_in_MIDP_en.pdf
[246] http://www.mysecured.com/?p=127
[247] https://securityinabox.org/es/chapter-10
[248] https://securityinabox.org/en/Glossary#GPS
[249] https://securityinabox.org/es/chapter-5
[250] https://securityinabox.org/es/Glossary#FOSS
[251] https://securityinabox.org/es/glossary#GPS
[252] https://securityinabox.org/en/android_basic
[253] http://f-droid.org
[254] https://securityinabox.org/en/glossary#FOSS
[255] https://securityinabox.org/en/glossary#apk
[256] https://securityinabox.org/es/chapter_10_2
[257] https://securityinabox.org/es/chapter_10_2_2
[258] https://securityinabox.org/en/Glossary#VoIP
[259] https://securityinabox.org/en/glossary#skype
[260] https://securityinabox.org/es/chapter_7_3
[261] http://f-droid.org/repository/browse/?fdid=com.csipsimple&fdpage=4
[262] https://guardianproject.info/wiki/OSTN
[263] https://ostel.me
[264] https://guardianproject.info
[265] https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone
[266] https://securityinabox.org/es/chapter_10_2_3
[267] https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms
[268] https://securityinabox.org/es/textsecure_principal
[269] https://guardianproject.info/apps/gibber/
[270] https://securityinabox.org/en/glossary#OTR
[271] https://securityinabox.org/es/gibberbot_principal
[272] https://chatsecure.org
[273] https://securityinabox.org/en/glossary#Tor
[274] https://securityinabox.org/en/apg_main
[275] https://code.google.com/p/cryptonite/
[276] https://securityinabox.org/es/chapter_11_7
[277] https://securityinabox.org/en/Cryptonite_main
[278] https://securityinabox.org/en/keepassdroid_main
[279] https://securityinabox.org/es/chapter_7_1
[280] https://securityinabox.org/es/chapter-7
[281] https://securityinabox.org/es/APG_principal
[282] https://securityinabox.org/es/K9_APG_principal
[283] https://guardianproject.info/apps/obscuracam/
[284] https://securityinabox.org/es/Obscuracam_principal
[285] https://www.witness.org
[286] https://www.torproject.org/docs/android.html.en
[287] https://securityinabox.org/es/Orbot_principal
[288] https://securityinabox.org/es/Orweb_principal
[289] https://securityinabox.org/en/glossary#Firefox
[290] http://f-droid.org/repository/browse/?fdid=org.mozilla.firefox
[291] https://guardianproject.info/apps/proxymob-firefox-add-on/
[292] https://guardianproject.info/
[293] http://www.cyanogenmod.com
[294] http://www.cyanogenmod.com/devices
[295] http://www.whispersys.com/
[296] http://www.whispersys.com/whispercore.html
[297] https://help.riseup.net/en/vpn
[298] https://support.apple.com/kb/HT1424