

CryptoPeriodismo

Manual Ilustrado Para Periodistas

nelson fernandez

Pablo Mancini

*Un paranoico es alguien que sabe
un poco de lo que está pasando*

William S. Burroughs

Índice

1. Prólogo: Una brújula para periodistas, por Andrés D'Alessandro
2. Introducción
3. Cómo generar contraseñas seguras
4. Cómo gestionar claves
5. Cómo armar un sistema de correos no vinculante
6. Cómo encriptar el contenido de los chats
7. Cómo anonimizarse al usar Internet
8. Cómo construir un túnel privado
9. Cómo tener una privacidad "bastante buena"
10. Cómo asegurar su teléfono
11. Cómo encriptar un disco
12. Nos vemos en el café de la esquina

Prólogo: Una brújula para periodistas

Todas las cosas son palabras del idioma en que Alguien o Algo, noche y día, escribe esa infinita algarabía que es la historia del mundo. En su tropel

pasan Cartago y Roma, yo, tú, él, mi vida que no entiendo, esta agonía de ser enigma, azar, criptografía y toda la discordia de Babel.

Detrás del nombre hay lo que no se nombra; hoy he sentido gravitar su sombra en esta aguja azul, lúcida y leve, que hacia el confín de un mar tiende su empeño, con algo de reloj visto en un sueño y algo de ave dormida que se mueve.

"Una brújula", Jorge Luis Borges

A la espalda de Winston, la voz de la telepantalla seguía murmurando datos sobre el hierro y el cumplimiento del noveno Plan Trienal. La telepantalla recibía y transmitía simultáneamente. Cualquier sonido que hiciera Winston superior a un susurro, era captado por el aparato. Además, mientras permaneciera dentro del radio de visión de la placa de metal, podía ser visto a la vez que oído. Por supuesto, no había manera de saber si le contemplaban a uno en un momento dado. Lo único posible era figurarse la frecuencia y el plan

que empleaba la Policía del Pensamiento para controlar un hilo privado. Incluso se concebía que los vigilaran a todos a la vez. Pero, desde luego, podían intervenir su línea cada vez que se les antojara.

"1984", George Orwell

La ficción, qué duda cabe, se anticipó de manera profética innumerables veces a la realidad. Y no sólo en lo que se refiere a cuestiones tecnológicas o científicas, sino también (y más bien) a aspectos sociológicos y filosóficos. 1984, la fantástica novela distópica que publicó George Orwell en 1949, debe ser uno de los textos más citados y divulgados de la historia contemporánea. Por la academia y por la calle; en sesudas tesis universitarias y también en anodinos paneles televisivos.

A pesar de que Orwell habló de telepantallas y jamás imaginó algo parecido a una red de redes (ese mérito en la ficción podríamos adjudicárselo a Murray Leinster, Fredric Brown, Isaac Asimov o William Gibson), con su nihilismo y desencanto logró predecir algunas de las características más riesgosas que configura Internet: su ubicuidad y omnipresencia (¿policial?).

Esa mirada paranoide es también la primera sensación que despiertan ya desde la Introducción Nelson Fernández y Pablo Mancini cuando explican por qué y para qué hacer un Manual Ilustrado de *CryptoPeriodismo*. ("Si algo es fácil actualmente es monitorear y espiar las actividades de un periodista", nos alarman). Pero, por suerte para el lector, su mirada no se agota en el pesimismo inicial cuando describen con información y sin mitología la

militarización de la Red en el mundo y cómo nos espían en la Argentina, temas que deberían (preo)ocuparnos más a periodistas, blogueros, defensores de derechos humanos, abogados, intelectuales, políticos, académicos, etc.

Internet, las redes sociales y las herramientas digitales son aliados fundamentales para la tarea profesional de los periodistas. Trabajemos en el formato que trabajemos, medios tradicionales o nuevos medios, el ecosistema digital nos sorprende cada día con novedades y nuevas posibilidades.

Sin embargo, los periodistas tenemos la obligación de ser conscientes de los riesgos crecientes que también aparecen en el horizonte con el uso de las nuevas tecnologías digitales. En eso se basan los autores del Manual para convencernos de que periodistas y medios debemos adaptarnos a esta nueva realidad sin volvernos (tan) paranoicos.

Por la lógica y los procedimientos profesionales que se involucran en nuestra tarea, y por los valores éticos y la responsabilidad social que implica en la relación que tenemos con los ciudadanos en un sistema democrático, los periodistas debemos necesariamente conocer y asumir como parte de nuestra actividad cotidiana los nuevos peligros a los que nos exponemos. Peligros que directa y/o indirectamente pueden afectar tanto a la materia prima con la que trabajamos, la información, las fuentes, los documentos, así como a nuestra reputación y a la de los medios en los que trabajamos, y a nuestros colegas.

En la paranoia orwelliana cualquier sonido o movimiento de los habitantes de "Oceanía" era

registrado y escuchado por la Policía del Pensamiento, y luego ese "hilo informativo" permitía a los funcionarios del Partido Único apresar, torturar y doblegar moralmente a los díscolos o rebeldes como Winston Smith, para que, traicionados y derrotados, acepten la "verdad" impuesta por el Gran Hermano.

Para vencer esa persecución permanente, dice Orwell casi al comienzo de su novela, los "proles" tenían que vivir con la seguridad de que todos sus movimientos serían observados, y con la certeza de que ese hábito finalmente se terminaba convirtiendo casi en un instinto de supervivencia.

Este Manual es una brújula, que permite señalar en varias direcciones los hábitos que deberíamos asumir los periodistas como seguras salidas al laberinto que presenta el uso (y abuso) de la tecnología, seamos expertos o ignaros. Con sutiles diferencias respecto del mundo que pinta Orwell, pero con la presencia de ciertos mecanismos perfeccionados de control y espionaje que hubiesen asustado aún más al autor inglés.

Asuntos casi siempre complejos como generar contraseñas seguras, gestionar claves, armar sistemas de correos no vinculantes, encriptar el contenido de los chats y de los discos, anonimizar el uso de Internet, asegurar el uso de los teléfonos celulares, etc. aparecen explicadas paso a paso en el Manual de *CryptoPeriodismo* e ilustradas de una manera didáctica y comprensible, aplicable para periodistas de todo el mundo.

Mancini y Fernández, especialistas en el tema, ofrecen con amplia generosidad toda su experiencia, claves, pistas, atajos, vericuetos y soluciones para

que periodistas y medios de todas las latitudes entendamos y nos adaptemos a esta nueva realidad.

Andrés D' Alessandro.

Director Ejecutivo del Foro de Periodismo Argentino (Fopea.org). Licenciado en Ciencias de la Comunicación (UBA).

Introducción

Nunca en la historia la humanidad tuvo tantas herramientas disponibles para comunicarse. El periodismo, como muchas otras profesiones, es beneficiario directo de las nuevas formas de comunicación que la evolución tecnológica está haciendo posible. Desde hace tres décadas, las tecnologías digitales auspician una transformación de proporciones industriales para la actividad de los medios y el trabajo de los periodistas. Toda una constelación tecnológica viva de nuevos equilibrios productivos está empujando hacia una reorganización sin precedentes de las formas de ejercer el periodismo.

A principios de los años noventa, los medios de comunicación aprovecharon la ventana de oportunidad abierta cuando la Web comercial irrumpió en la vida de cientos de miles de personas. Inmediatamente y en todo el mundo, las ediciones digitales de los diarios especialmente, se convirtieron en los sitios más visitados de la Red.

El cambio de milenio encontró a la Web evolucionando de una plataforma de consulta hacia un ecosistema de participación popular. Los primeros blogs ya estaban en línea. Proyectos hoy consagrados como la Wikipedia y Wikileaks eran entonces ideas funcionando en los cerebros de sus creadores. Los negocios digitales de la época, la publicidad online y el comercio electrónico, colapsarían con el derrumbe financiero que representó la explosión de la burbuja de las puntocom para luego rediseñar y diversificar sus modelos de crecimiento como los conocemos en el 2013.

Con servicios como Amazon y Google funcionando, todavía eran impensables "game changers" como Youtube, Facebook o Twitter, que también tendrían un impacto directo en la profesión periodística, la distribución de contenidos, la relación con las fuentes y la disponibilidad de información a escala planetaria. Menos imaginables eran entonces novedosas criaturas mediáticas como The Huffington Post y productos que rediseñarían la relevancia de las voces autorizadas sobre temas específicos como Trip Advisor.

A principios de este siglo, con distintos niveles de aceleración según las regiones del mundo que se analicen, los periodistas comenzaron a adoptar cada vez más tecnologías en sus vidas personales y para su desarrollo profesional. Se armaron de dispositivos, de herramientas y con infraestructura.

Todo cambio industrial y cultural profundo siempre engendra apocalípticos e integrados. Los medios digitales no fueron ni son la excepción. Si bien todavía tienen lugar las discusiones sobre el valor destruido y el valor creado en el periodismo, a partir del desarrollo de las tecnologías digitales en ambos bandos anida un acuerdo cada día más sólido: el periodismo se enfrenta actualmente a los peligros del siglo XX, como la persecución, la censura y el asesinato de profesionales, mientras que también debe lidiar con un nuevo conjunto de peligros que facilita el ambiente tecnocultural de principios del siglo XXI, como el espionaje, la vigilancia y el monitoreo que ejercen gobiernos y empresas de todo el mundo sobre las comunicaciones de los periodistas.

Las oportunidades, los beneficios y los desafíos que representa el cambio tecnológico para la profesión

periodística y para los medios de comunicación han sido comentados, discutidos y analizados en miles de libros publicados durante la última década. Pero poco se ha dicho sobre los nuevos peligros a los que está expuesto el conjunto de trabajadores de la prensa. Quizás porque nunca a nadie le consta -hasta que se vuelve una víctima- cuánto hay de cierto, cuánto de leyenda o fantasía, cuánto de posible y cuánto de ciencia ficción, a la hora de entender los riesgos del nuevo escenario profesional.

La Red se está militarizando

Ésta es la era del registro. El espionaje y la vigilancia jamás tuvieron las cosas tan fáciles. Nunca fue un mercado tan rentable. No sólo es posible y tecnológicamente cada vez más preciso: ostenta un alcance insospechado hace sólo unas décadas. Una industria creciente de inteligencia, máquinas y software está en plena expansión y crecimiento. Y esta industria es, por definición, invisible y silenciosa.

Las soluciones de interceptación masiva de información y almacenamiento, como las de análisis semántico de grandes volúmenes de datos, se expanden al ritmo que gobiernos y corporaciones contratan esos servicios. Los seis principales segmentos de mercado son: monitoreo de contenido y tráfico de internet, monitoreo de comunicaciones móviles (llamadas), monitoreo de SMS, trojanos en dispositivos, análisis semántico de contenido de comunicaciones y trackeo por GPS. Los contratistas principales de las agencias de inteligencia y fuerzas militares de decenas de países, son proveedores de estas tecnologías. Algunos de ellos son: VASTech, Gamma Corporation, Amesys, ZTE Corp, SS8,

Hacking Team, Vupen, Phoenexia, Blue Coat, y la lista continua. En el 2012, los principales clientes fueron Libia, Egipto, Ucrania, Turquía, Sudáfrica, Hungría, China, Colombia, Brasil, Canadá, Estados Unidos, Reino Unido, España, Suiza, Rusia, Italia, India, Alemania, Francia, entre otros países.

Internet es una infraestructura invisible en todos los aspectos de nuestra vida. El espionaje es un hecho constante y, por definición, masivo. El espionaje versión siglo XXI se lleva a cabo monitoreando grandes volúmenes de comunicaciones. No es personalizado. Esto nos convierte a todos en potenciales víctimas. Sólo después de espiar a todos, es posible individualizar y espiar a algunos. Ahora la vigilancia es, además, retroactiva. Durante la Guerra Fría el espionaje fue dirigido: primero era Usted sospechoso y sólo entonces se procedía a monitorear su vida. Ahora las cosas cambiaron: todos estamos vigilados y cuando alguien se convierte en sospechoso se rastrea toda la información al alcance que haya sido capturada y almacenada previamente. La vigilancia del siglo pasado, dirigida, y ejercida físicamente por humanos organizados en turnos y de forma presencial, sigue teniendo vigencia, pero está obsoleta comparada con las posibilidades y la eficacia que actualmente ofrece la tecnología.

El periodismo es sólo una víctima más de esa realidad. Para dar un ejemplo ilustrativo: existen máquinas subacuáticas para espiar las comunicaciones digitales de poblaciones enteras. Empresas que fabrican y venden robots que se sumergen para interceptar los cables de fibra óptica y los repetidores tendidos en el fondo del océano que propulsan la mayor parte de las comunicaciones digitales por todo el mundo. Empresas venden ese servicio y otras empresas y gobiernos de

todo el mundo los compran. Incluso países con muy pocos recursos, algunos muy pobres, invierten parte de su presupuesto en estas tecnologías.

Pero mucho más cerca, en los bolsillos de las personas también existe un riesgo probable. Escuchar y rastrear llamadas de teléfonos celulares no sólo es posible: es muy fácil y muy barato. Del mismo modo que cualquier persona investigando un poco puede publicar una página en Internet, también puede comprender cómo interceptar comunicaciones y hacerlo con destacada eficiencia. Un ejemplo contundente: países con muy pocos recursos, como Libia, pueden pagar por tecnologías de monitoreo. Se invierten sumas menores, insignificantes, de dinero para tener acceso a tecnología de alta eficiencia para interceptar redes GSM. Por un millón de euros se pueden comprar esos sistemas de monitoreo de telefonía.

La Red es una fábrica de huellas y rastros, un catálogo de comunicaciones, conexiones y actividades individualizables, geolocalizables. Si una comunicación es digital es también interceptable, monitoreable. Todavía, la única forma de reducir al máximo posible las probabilidades de espionaje sobre una comunicación es conversar caminando, con el teléfono celular en un bolsillo y con su batería en el otro. Esa es la opción menos insegura: conversar caminando y con el teléfono sin batería. O mejor: sin llevar el teléfono.

La Red es una extensión de la complejidad de la sociedad como sistema. Del mismo modo que en su arquitectura las más nobles expresiones de colaboración cultural y organización social encuentran renovadas formas de funcionamiento, en la Red también habitan las más repudiables formas de represión contra la libertad

de información, la transparencia, la privacidad y contra las libertades en general. Es iluso pensar que la Red importa lo mejor de las sociedades analógicas. Lo peor también es parte de lo que ofrece. La Red es la mayor y más eficiente arquitectura conocida de vigilancia.

La Red no sólo expresa nuevas formas de libertad. También se vuelve una extensión real de la vigilancia y la militarización de la sociedad. Toda paranoia es justificada en un mundo en el que las armas, la represión y la censura del siglo XX desarrollaron extensiones virtuales y transparentes para esperar a sus víctimas en los nuevos entornos de circulación de información. Las armas de destrucción cultural masiva del siglo XXI son invisibles, a veces incluso en apariencia amigables, pero no menos poderosas, represivas y repudiables que las del siglo pasado.

Los peligros y riesgos históricos de ejercer el periodismo estuvieron asociados a las amenazas contra la integridad física. Generalmente se evitaron eludiendo zonas de conflicto. Los nuevos riesgos para la prensa no tienen tiempo ni territorio. El ciberespacio no tiene un mapa del horror. Su naturaleza lo hace inasible e intrínsecamente peligroso.

La dialéctica de la palabra VS. la espada, lamentablemente, todavía tiene vigencia. Pero es incompleta para entender cómo funciona realmente el mundo y cuáles son los riesgos a principios del siglo XXI.

La única forma de prevenir peligros intangibles, como la vigilancia, el espionaje y el monitoreo, de reducir sus probabilidades, es desarrollar una

protección tan inmaterial y a la vez tan poderosa que necesariamente debe estar basada en el mismo recurso que los hace posibles: el conocimiento.

Argentina: Nos espían

Este libro no se limita al trabajo de los periodistas argentinos. No obstante, el origen de esta publicación vuelve oportuno comentar el estado de la vigilancia que se ejerce en este país.

En el oficialismo y en la oposición tienen una relación esquizofrénica con la información: para discutir sobre medios y periodismo se anotan todos, pero de la transparencia de la información pública y de la privacidad de las personas no se encarga nadie.

El megaproyecto espía kirchnerista empezó ambicioso y truncado. En el 2004, Néstor Kirchner estableció por [decreto](#) la captación, conservación y derivación de los contenidos de las comunicaciones para su observación remota. Mediante el decreto 1563 pretendió que las empresas de telecomunicaciones inviertan millones de dólares en tecnología de vigilancia, escucha y monitoreo. El decreto era tan delirante que en el 2005 [se suspendió su aplicación](#), en parte por lobby de las propias "telcos" que no estaban dispuestas a invertir las sumas siderales que demandaba espíar por decreto a toda la población.

En el 2006 se reactivó el funcionamiento del Proyecto X, creado en el 2002 y del que en el 2012 se tomó conocimiento público: "Un sistema informático de inteligencia criminal para la investigación de delitos complejos. Es una base de datos con vinculadores que

permiten entrecruzar información y acelerar el análisis en determinadas circunstancias”, según lo definió la ministra de Seguridad de la Nación, Nilda Garré. [El Proyecto X fue denunciado](#) porque su protocolo de actuación vulneraba derechos constitucionales.

No existe información pública sobre [dos programas clave](#): el SADI (Sistema de Adquisición y Diseminación de Imágenes) y el SARA (Sistema Aéreo Robótico Argentino), que tienen decenas de millones de pesos de presupuesto y entre otros objetivos la inteligencia, vigilancia y reconocimiento. Estamos hablando de tecnología que puede detectar a una persona a 14 km de distancia, reconocerla a 5 km e identificarla a 2,5 km. De película pero no en una película: ahí afuera.

Los [aviones no tripulados](#) (drones) están en auge en todo el mundo y el debate sobre su uso no puede darse sin información pública mínima porque, [tal como se advierte en la Revista de Publicaciones Navales](#), “este ingenio puede ser empleado tanto en operaciones militares como en el campo civil”.

La vigilancia masiva en la Argentina se oficializó como política de Estado en el 2011. El 8 de noviembre de ese año se publicó en el Boletín Oficial el [Decreto Nacional 1766/2011](#) del Poder Ejecutivo para crear el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS). El propósito del programa es claro: “Identificación de personas y rastros”. Es prácticamente inexistente la información pública sobre SIBIOS. Sólo es posible conocer el decreto. Sobre cómo se estructuran los datos que el Estado captura y almacena, con qué bases de datos los cruzan y bajo qué políticas de seguridad los almacenan, nada se sabe.

La tarjeta [SUBE](#), el Sistema Único de Boleto Electrónico, "un medio de pago simple y moderno", según lo define el Gobierno, es otro mecanismo de vigilancia efectiva en la Argentina. Permite pagar viajes en colectivos, subtes y estaciones de trenes adheridas a la Red SUBE en el transporte público del Área Metropolitana de Buenos Aires (AMBA). La tarjeta es personal y el Estado guarda toda la información sobre los recorridos que hacen los usuarios todos los días, asociándolos a la persona física. Para decirlo sin vueltas: el Estado sabe quién y cuándo viaja desde qué lugar y hacia dónde, cada vez que usa la tarjeta. La información que captura y almacena es tan vulnerable que el 20 de enero del 2012 un grupo de hackers de la red Anonymous publicó la base de datos de SUBE en Internet para demostrar cómo el Estado está vigilando a los usuarios y la precariedad con la que protege la información.

Otros dos hechos llamativos son la compra de tecnología de espionaje para monitorear comunicaciones. En el 2010, un sistema para intervenir redes GSM a la empresa alemana Rohde & Schwarz y, en el 2012, un repetidor de microondas a China National Electronics Import and Export Corp. Sólo en esas dos tecnologías el Estado invirtió más de 2 millones de dólares.

La militarización de las comunicaciones es un proceso en alza en todo el mundo. También en la Argentina. El contexto local de transparencia ausente, de información pública que tiende a cero y de privacidad en peligro, vuelve todo más turbio y menos confiable. El decreto del 2004 para espionar a toda la población está suspendido. Pero hay indicios de que nos espían.

La transparencia es para los gobiernos y los estados. La privacidad para los individuos. No al revés.

El problema que resuelve este libro

Si algo es fácil actualmente es monitorear y espiar las actividades de un periodista. El problema es identificable: la mayoría no sabe cómo proteger sus comunicaciones, especialmente aquellas mediadas por Internet. El espionaje del que muchos están siendo víctimas es cada vez más obscuro, y es probable que se deba mucho más a la falta de conocimiento que a la supuesta súper inteligencia y a los inigualables recursos materiales de quienes espían.

Si un periodista hace un uso corriente de las tecnologías y no cuenta con nociones y herramientas elementales para reducir la vulnerabilidad de la seguridad de sus comunicaciones, está haciendo mal una parte de su trabajo. No sólo se expone y expone a la organización para la cual trabaja, además, puede poner en riesgo la seguridad de sus fuentes y la de sus colegas.

La Red siempre parece lo suficientemente amplia, extensa, ancha, diversa y desconocida como para que alguien pueda "tomarse el trabajo de encargarse de nosotros y de nuestras comunicaciones". Pero puede pasar. Es más, es probable que Usted ya haya querido tener acceso a la información de otras personas, y que otras personas hayan querido, o incluso intentado, tener acceso a la suya. Si es que ya no la tienen. Lo único que diferencia a unos de otros es el conocimiento y la ética. El deseo, iguala.

Así las cosas, no se trata de convertirse en genios de la criptografía ni en matemáticos especializados en blindar y cifrar con algoritmos complejos las comunicaciones. Se trata, sí, de tener al alcance algunas herramientas que contribuyan a una experiencia lo más segura posible en un ambiente naturalmente inseguro. Es por eso que este libro no es un manifiesto de resistencia al espionaje ni un catálogo de casos sobre cómo grandes organizaciones y gobiernos monitorean actividades y comunicaciones de medios y periodistas. Es un documento básico sobre cómo estar menos inseguros frente a esa, ya no amenaza sino, realidad.

Los esfuerzos y recursos utilizados para limitar al periodismo no son sólo aquellos que pretenden silenciarlo. En buena parte de los casos no se pretende detener al periodismo sino dejarlo funcionar y monitorearlo desde muy cerca. Como no es posible controlar o detener la circulación de la información, en la actualidad las estrategias de espionaje están orientadas a objetivos de anticipación política. Es muy difícil, es imposible por la naturaleza distribuida de la Red, tener control de la información que está circulando, pero sí es posible saber qué circula y quiénes están detrás de esa distribución, y probablemente se podrán planificar acciones tácticas para relativizar su impacto o intentar desviar la atención.

La maquinaria de espionaje no descansa y su funcionamiento eficiente es, por definición, no restrictivo sino silencioso. No reactivo sino retroactivo. No individual ni dirigido sino masivo.

Cuando Usted termine de leer este libro podrá saber lo inseguro que estaba hasta antes de leerlo. Este libro no le ofrece garantías de que no puedan espiarlo. Pero sí le ofrece herramientas para que quienes pretendan hacerlo tengan las cosas más difíciles.

Sobre el libro

El objetivo de este libro es ofrecer de un modo simple y práctico herramientas y soluciones que contribuyan a reducir el peligro que corren los periodistas en el ciberespacio y cuando establecen comunicaciones mediadas por tecnologías digitales.

Muy lejos de ofrecer métodos y técnicas infalibles, *CryptoPeriodismo* ofrece procedimientos que, combinados, pueden proteger el trabajo y la seguridad de los periodistas.

Es un instrumento preventivo. Ofrece información e instrucciones que reducen sensiblemente las probabilidades de espionaje, pero, de nuevo, no es infalible. La naturaleza de la evolución tecnológica limita inevitablemente el alcance de estas sugerencias. Por la misma razón, este manual ilustrado es provisorio. Sirve, entonces, parcialmente, ahora. No sabemos mañana, ni dentro de unos años. Con toda probabilidad demande actualizaciones periódicas que, esperamos, surjan de la experiencia y del conocimiento de colegas que tengan la intención de colaborar con su actualización.

En ese sentido, hacemos devolución expresa de los contenidos de este libro al dominio público, para que cada uno de Ustedes pueda usarlo del modo que considere más conveniente.

Agradecemos a Mariella Miranda que diseñó la tapa y a Andrés D'Alessandro que escribió el prólogo.

Buenos Aires, 15 febrero del 2013.
Pablo Mancini, nelson fernandez.

Cómo generar contraseñas seguras

Las claves de acceso a los dispositivos y a los servicios Web son, frecuentemente, una fuente de problemas. Implican una gestión difícil y es muy fácil terminar simplificándolas, y consecuentemente corriendo riesgos serios para poder recordarlas. Son puertas de acceso que, una vez abiertas por terceros, no hay nada que hacer excepto, en el mejor de los casos, esperar a volver a tomar el control pero habiendo perdido información y, sobre todo, privacidad.

Las claves que Usted usa a diario representan dos desafíos de seguridad: cómo diseñarlas y cómo gestionarlas. Una buena combinación de diseño y gestión de claves reduce sensiblemente las probabilidades de que un dispositivo o un servicio Web sea vulnerado, aunque es claro: nada es 100 % seguro.

Quienes intentan violar contraseñas ajenas frecuentemente lo hacen mediante tres métodos bien diferenciados, de complejidad variable y aplicados a distintos contextos: [ataques de diccionario](#), [ingeniería social](#) y acceso físico a un dispositivo.

Un ataque de diccionario es un método de [cracking](#) basado en la "fuerza bruta". Es poco inteligente pero no por eso poco efectivo. Consiste en averiguar contraseñas probando múltiples combinaciones de caracteres miles de veces hasta dar con la correcta. Un robot genera las combinaciones e intenta acceder con cada una de ellas. Hasta que no encuentra aquella que busca y le permite acceder, no se detiene.

La ingeniería social es otra de las tres grandes compuertas para vulnerar contraseñas. Es una práctica

para obtener información sobre la víctima y, a partir de ella, dar con la clave que se busca o tener los datos que permiten recuperarla. El método actualmente está en pleno auge ya que la cantidad de información personal que se hace pública a diario en las redes sociales está creciendo de un modo inconmensurable. En las redes sociales circula la materia prima con la que se produce buena parte del espionaje actual.

El acceso físico a un dispositivo es un riesgo también creciente. Cada vez usamos más dispositivos conectados a la Red. Todos. Y todo parece indicar que esa tendencia continuará en ascenso durante los próximos años. La mayoría guarda contraseñas en sus dispositivos. Los navegadores de las computadoras y las aplicaciones de los dispositivos móviles son verdaderos paraísos para el espionaje. El acceso físico muchas veces es la llave maestra que abre todas, o casi todas, las demás puertas.

En esta parte del libro ofrecemos algunas sugerencias para crear y gestionar claves de un modo seguro, que reduzcan al mínimo las probabilidades de ser conocidas y usadas por terceros.

Paso a paso

Para empezar, lo esencial es descartar la estrategia de la memoria fácil: fechas de nacimiento, números de documentos de identidad o pasaporte, números de teléfono, apodos, nombres de parientes y mascotas, direcciones de lugares que puedan ser asociadas con Usted, edad, ciudades, barrios, códigos postales, etc. Toda esa información es demasiado predecible. Descartarla a la hora de crear contraseñas equivale a

dejar fuera de juego la posibilidad de que alguien con tiempo, cercano a Usted o un desconocido con acceso a información sobre Usted, se tome el trabajo de intentar "adivinar" sus passwords y, con un poco de suerte, acertar. De hecho, existen servicios Web que solicitan ese tipo de información. En ese caso, lo más recomendable es no usarlos. Si no tiene más opción que hacerlo, mienta: no publique su dirección, teléfono o código postal, por ejemplo.

Su segunda misión es sacarse de la cabeza que es algo seguro usar la misma clave de acceso para todo. De hecho esa estrategia implica todo lo contrario: es lo más inseguro que Usted puede hacer.

Un algoritmo para crear passwords seguras puede ser el siguiente:

1. Usted, como todos nosotros, recuerda una frase o título de un libro, el estribillo de una canción, una cita, una película, etc. Lo primero que debe hacer es seleccionar aquella frase que recuerda con precisión pero que no lo representa ante su entorno social. Es decir, aquella que sabe que es muy improbable que pueda ser asociada con Usted.

2. Una vez identificada esa frase debe seleccionar solamente una letra de cada palabra que la compone. Pongamos por ejemplo, la primera letra. Aunque lo más recomendable sería que use la segunda, o la tercera, etc., o una combinación. Por ejemplo, si la frase que eligió es "Nunca sería socio de un club que me aceptara como miembro", el nemónico tomando la primera letra de cada palabra sería "nssducqmacm". Ya dio un primer paso, está más lejos de la inseguridad. Pero vaya más allá.

3. Añada una variable más, una letra en mayúsculas. La tercera por ejemplo: "nsSducqmacm".

4. Tome en cuenta el servicio Web para el que está creando esa clave, por ejemplo "mail.google.com". Elija la marca o alguna palabra con la que Usted lo asocie mentalmente. Si es la marca, en este caso, sería "google". Si es una palabra, podría ser "correo". Ahora complete su contraseña: una esta variable a la clave generada en los tres puntos anteriores con un signo, por ejemplo, "!". El resultado es "google!nsSducqmacm" o bien "correo!nsSducqmacm".

5. Un último agregado para terminar de crear su clave: añada un número y otro símbolo. Por ejemplo ";12". Su contraseña es ahora: "google!nsSducqmacm;12" o bien "correo!nsSducqmacm;12".

Ahora bien, esta clave le permitirá acceder a su cuenta de correo en Google. Modifíquela para cada servicio extra que use. Por ejemplo, para su clave de Twitter, podría ser: "Twitter!nsSducqmacm;12".

Siguiendo estos cinco pasos es posible crear una contraseña fuerte a nivel de seguridad y relativamente simple de recordar. El método reduce el margen de inseguridad pero no es infalible. Si al servicio al que Usted está accediendo con esta clave no la almacena de un modo seguro, su clave es tan vulnerable como si fuera "1234567890"

Cómo gestionar claves

Crear passwords seguras es sólo un primer paso. Usted ahora debe contar con alguna herramienta para

minimizar el riesgo de que alguien pueda acceder a sus claves y, en caso de que sea accedida por un tercero, no pueda usarla. Lo que debe hacer es aplicar un algoritmo de hash su clave.

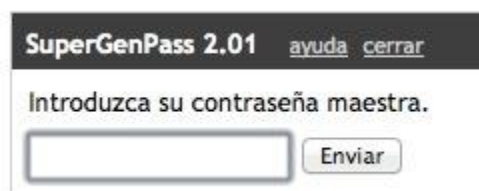
A las [funciones hash](#) (adopción más o menos directa del término inglés *hash function*) también se las llama funciones picadillo, funciones resumen o funciones de digest. El término *hash* proviene de la analogía con el significado estándar de dicha palabra: *picar y mezclar*.

En la gestión de claves, un Hash es un algoritmo que se aplica sobre un texto (también puede ser usado sobre otros formatos de archivos, como .mp3 o formatos de video). A partir de ese texto, genera un número que identifica a ese texto, a esa clave. La longitud del número va a depender de la función de digesto que utilice. Las más comunes son [MD5](#) y [Sha1](#). Aplicar esto a sus claves construye un obstáculo más para el tercero que busque conocerlas. Es decir, cuando ese tercero encuentre su clave, en realidad no encontrará otra cosa que un número compuesto aproximadamente por veinte caracteres. Usted construyó ese número aplicando un Hash sobre su password, pero la persona que se encuentre con ese número, será incapaz de conocer su clave a partir de esa cifra.

Suena complejo pero es muy simple de poner en práctica este método de seguridad. Existe un servicio llamado [SuperGenPass](#) que está implementado como un [bookmarlet](#) y por tanto se ejecuta completamente en su navegador sin utilizar ningún sitio externo, sin compartir datos, nada. Cuando se lo invoca, se requiere ingresar una password maestra, que es la única clave que Usted debe recordar y automáticamente genera la clave para el sitio que se va a acceder. El servicio

utiliza más o menos el mismo algoritmo explicado anteriormente y le agrega la función de hash. Con lo cual, si el servicio que está utilizando no guarda sus claves de forma segura, no importa, ya que Usted está enviando una clave en un formato seguro.

Al invocar el bookmarklet se le solicitará ingresar una contraseña maestra utilizada para generar la clave para el sitio:



The screenshot shows a web interface for SuperGenPass 2.01. At the top, there is a dark header with the text "SuperGenPass 2.01" and two links: "ayuda" and "cerrar". Below the header, the main content area has the text "Introduzca su contraseña maestra." followed by a text input field and a button labeled "Enviar".

Y luego le presentará la contraseña generada para el sitio que se está visitando:



The screenshot shows the SuperGenPass 2.01 interface after password entry. The header is the same as in the previous screenshot. The main content area is divided into three sections: 1. "Su contraseña generada" with a text input field containing ten asterisks and a link "mostrar/ocultar" below it. 2. "Su contraseña maestra" with a text input field containing four asterisks and a link "mostrar/ocultar" below it. 3. A footer section with the text "Regenerar contraseña" and a link "mostrar/ocultar".

Utilizando los links de 'mostrar/ocultar' se puede acceder a toda la información que utiliza el bookmarklet para generar la contraseña:

Your generated password

k6aNrHOxKv

[show/hide](#)

Your master password

prueba

[show/hide](#)

Regenerate password [show/hide](#)

Master password

••••••

Domain / URL

supergenpass.com

Disable subdomain removal

Password length

10

Submit

Cómo armar un sistema de correos no vinculante

Los correos electrónicos son actualmente un mecanismo clave de la comunicación y una herramienta, sino *la* herramienta, que periodistas usan a diario para comunicarse. El mundo es más comfortable con emails que sin emails, pero vale decir también que las comunicaciones son sensiblemente más vulnerables cuando los emails entran en juego. Es por ello que Usted debería tomar todas las medidas de seguridad a su alcance.

Construir un sistema de correos no vinculante es fácil y contribuye a minimizar la inseguridad de sus intercambios electrónicos.

Uno de los problemas centrales respecto de los emails es que cuando alguien tiene acceso a su cuenta de correo, accede virtualmente a mucho más: redes sociales, compras, servicios vinculados a los bancos con los que Usted opera, agenda de actividades, calendario de trabajo persona, chats, en fin... De todo.

El propósito concreto de crear un sistema de correos no vinculante es que si alguien logra acceder a su cuenta de correo electrónico, no podrá encontrar información que le permita continuar violando su privacidad y consiguiendo más información sobre Usted. Se trata, entonces, de evitar que acceder a su email sea una llave maestra para acceder a todo lo demás: servicios en la nube, cuentas bancarias y perfiles en redes sociales, entre muchas otras cosas.

Actualmente Usted está en peligro: si alguien tiene acceso a su cuenta de correo, está en el acto habilitado para tomar control de sus perfiles de Facebook, Twitter, Skype, Dropbox, o cualquier otro que utilice. Por razones profesionales, su email es público. Esta situación lo expone más que a cualquier otro usuario de sistemas de correos electrónicos.

El sistema de correos no vinculante parte de la premisa de que en algún momento alguien podría tomar control de su cuenta de correo electrónico principal. Esto es lo que debería hacer para minimizar los riesgos:

1. Su email público, es decir, aquel al cual le escriben sus contactos y personas que desean comunicarse con Usted, debe ser una cuenta "alias". Por ejemplo: si su email público es `periodista@ejemplo.com`, Usted debe convertir esa cuenta en un alias, y redirigir sus mails entrantes a otra cuenta, en otro dominio, por ejemplo a `periodista25@3j3mplo3.com`. Es en esta segunda cuenta, que debe ser secreta y nadie salvo Usted puede conocer de su existencia, Usted recibirá toda comunicación que sea enviada a `periodista@ejemplo.com`. Lo que deberá hacer también es configurar `periodista25@3j3mplo3.com` para que le permita enviar correos con el alias `periodista@ejemplo.com`, de tal forma que cuando Usted envíe un correo no revele la verdadera cuenta que está usando y siempre se muestre el alias.

Este primer paso hará que si alguien eventualmente logra ingresar a `periodista@ejemplo.com` se encontrará con nada. Eso sí, tendrá acceso a saber que Usted opera con la cuenta `periodista25@3j3mplo3.com`. Con lo cual Usted gana tiempo y el intruso deberá reiniciar el

proceso de espionaje. Por eso es tan importante que Usted registre su segunda cuenta en un servicio distinto a la primera, con datos falsos.

2. Su cuenta de correo real, no el alias, no puede estar vinculada a ningún otro servicio. Es por ello que Usted debería crear una cuenta de correo por cada red social o servicio que utilice. Esto tiene un aspecto en contra: recibirá notificaciones de esos servicios en distintas direcciones de email. Pero tiene un aspecto a favor: quien pueda ingresar a uno de esos servicios que Usted está utilizando, podrá tener accesos sólo a ese, y no a todos los demás. Esas cuentas que Usted creará para registrarse en los servicios que utiliza, deben ser secretas, no se las puede decir a nadie, y no deben tener ninguna coincidencia con su persona. Por ejemplo: Si su email público es `periodista@ejemplo.com`, que es un alias que Usted gestiona desde `periodista25@3j3mplo3.com`, su registro en Twitter debería hacerlo con una tercera cuenta que Usted cree para tal efecto, por ejemplo: `ptwsta.2le3t@gmail.com`.

Si alguien en este momento tuviese acceso a su cuenta en Gmail, por ejemplo, es muy probable que también tenga accesos a su cuenta de correo corporativa, a su perfil en Facebook, Twitter, Dropbox, bancos que utiliza, entre muchos otros servicios. Porque si alguien en este momento tuviese acceso podría recuperar las contraseñas de todos esos servicios reseteándolas. Y todas esas notificaciones de cambios de contraseñas llegarían, siguiendo con el ejemplo, a esa cuenta en Gmail. Es por esa razón que Usted necesita armar un sistema de correos no vinculante. Para que si alguien accede a A, no pueda acceder a B, ni a C, ni a D, etc.

Cómo encriptar el contenido de los chats

El chat es una puerta de inseguridad permanentemente abierta. Los periodistas usan servicios de mensajería instantánea todos los días, tanto para establecer comunicaciones personales como profesionales. En cualquier caso, exponen su comunicación y, algo nada menor, exponen a las personas con las que se comunican a través de mensajería instantánea.

Cuando del otro lado del chat hay una fuente o un colega, el riesgo aumenta exponencialmente. Llama la atención que buena parte de los profesionales sigan utilizando servicios como Google Talk o, peor, MSN. Están totalmente expuestos a ser espiados.

En investigaciones periodísticas y judiciales aparecen, cada vez más en carácter de evidencia, fragmentos de comunicaciones mediadas por software y pantallas. Un ejemplo concreto respecto de que en la Red nada, nada, nada de nada, es off the record. Todo es en On.

Haga la prueba, abra su cuenta de Google Talk, active la opción Off the record y converse con cualquiera de sus contactos. Luego de un par de mensajes enviados y recibidos, abra esa misma cuenta desde un teléfono o cualquier otro dispositivo. ¿Sabe qué verá? Toda la conversación. Así que cuidado: el Off the record de muchas aplicaciones no es tan off, y es bastante más on the record de lo que prometen. Copias de sus comunicaciones se replican en servidores permanentemente, en todo el mundo. Usted no tiene control de esa situación. Su única opción es no usar

esas aplicaciones. Y usar otras considerablemente menos inseguras como, por ejemplo, [Jabber](#).

Jabber es un protocolo de mensajería instantánea y presencia que fue estandarizado para Internet por el [Internet Engineering Task Force \(IETF\)](#) (Fuerza de Tareas de Ingeniería de Internet). Su denominación técnica es Extensible Messaging and Presence Protocol, más conocido como XMPP. Es abierto y extensible.

El proyecto Jabber comenzó a ser desarrollado en 1998 por Jeremie Miller. Actualmente, una de sus ventajas sustantivas es la seguridad. Los servidores XMPP pueden ser aislados de la red pública XMPP. Para apoyar la utilización de los sistemas de cifrado, la XMPP Standards Foundation pone a disposición de los administradores de servidores XMPP certificados digitales. Los estándares XMPP para clientes cuentan quince años después del comienzo de su desarrollo con diversas implementaciones. Lo usan, entre muchas otras, compañías como Sun Microsystems y Google.

La red XMPP está basada en servidores descentralizados; no hay ningún servidor central, a diferencia de otros servicios como AOL Instant Messenger o MSN Messenger.

Para su uso se requiere obtener una cuenta en un [proveedor del servicio](#) y utilizar algún [cliente que soporte el protocolo](#). Entre los clientes que podemos nombrar están:

Pidgin para Linux y Windows
<http://pidgin.im/>

PSI para Linux, Mac y Windows

<http://psi-im.org/>

Adium para Mac

<http://adium.im/>

Xabber para Android

<http://www.xabber.com/>

Gibber para Android

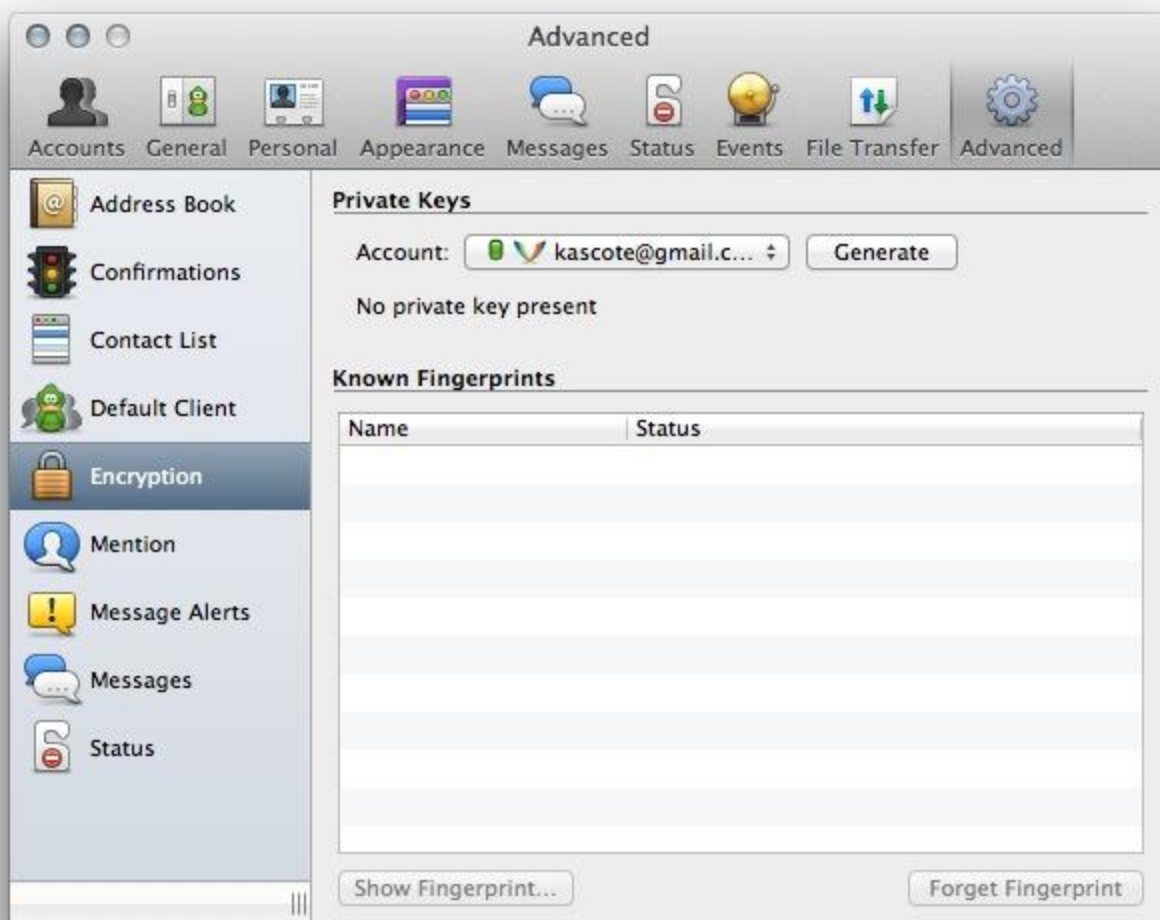
<https://guardianproject.info/apps/gibber/>

ChatSecure para iPhone

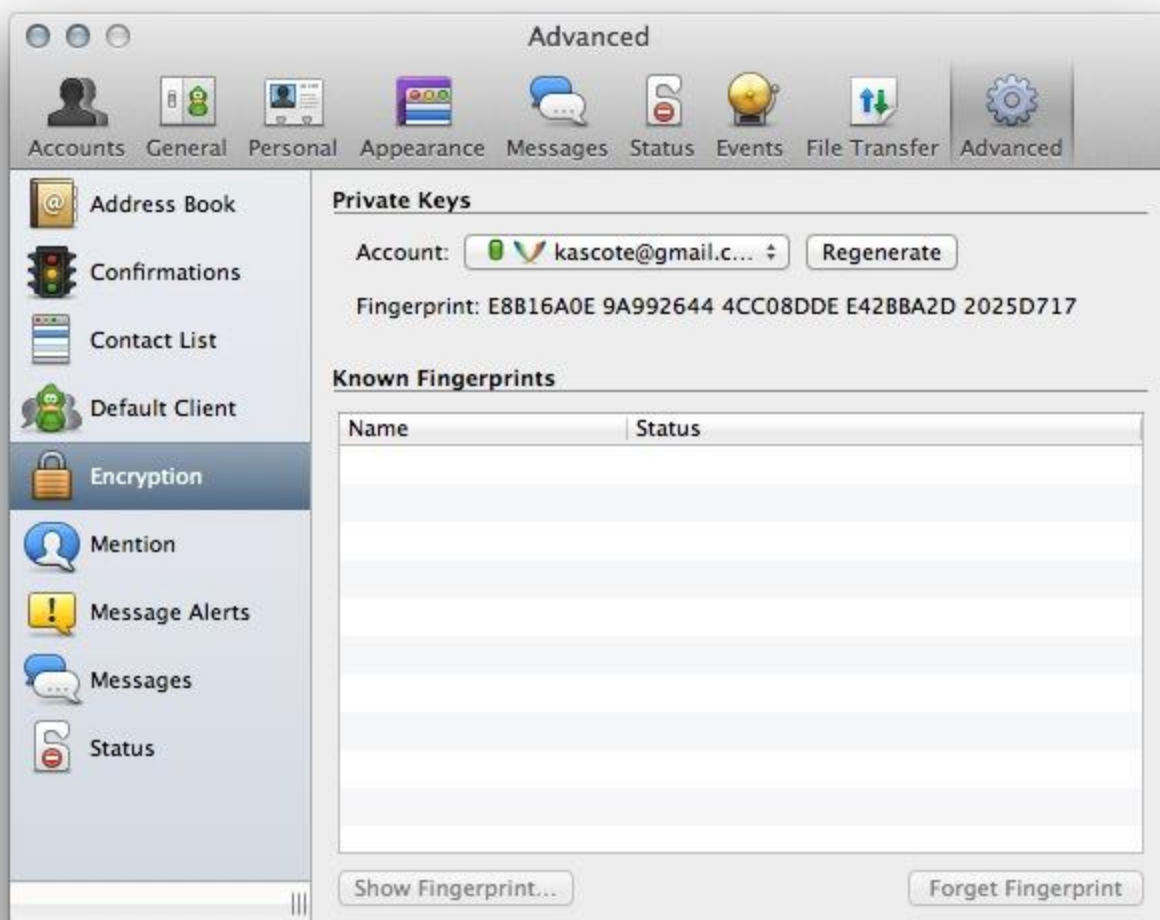
<http://chrisballinger.info/apps/chatsecure/>

Recomendamos utilizar XMPP y no MSN, Yahoo!, GTalk o Facebook u otro similar, debido a que distintos proveedores de XMPP tienen distintas políticas de privacidad, uso y servicio más relajadas y principalmente por el uso de plugins como [OTR \(Off the Record\)](#) que es lo que nos motiva en este libro. Mucho menos usar Whatsapp o BlackBerry Messenger: en ambas aplicaciones Usted renuncia a su privacidad y a saber qué hacen con sus datos y con la información que intercambia en esas herramientas de comunicación.

Para tener una comunicación segura con otra persona, no alcanza únicamente con que la conexión sea segura con el servidor utilizando el protocolo [SSL](#). Es necesario también que todo lo que se transmita entre las partes esté protegido y para eso sirve el plugin OTR. Este plugin permite encriptar todos y cada uno de los mensajes que son enviados y recibidos entre las partes que utilizan este plugin. Una vez instalado, lo que se debe hacer es generar una clave por cada cuenta donde se lo quiera utilizar. Esto es muy simple y sólo requiere la pulsación de un botón:



Una vez generada la clave, se va a mostrar su Fingerprint. Una buena práctica es verificar por otro medio (email, teléfono, SMS, etc.) el fingerprint de la persona con la que vamos a establecer la comunicación. Esta verificación se hará por única vez y es muy útil para asegurarnos de que no se trate de una cuenta impostada. El plugin tiene también una pantalla para administrar y dar de baja las distintas claves:



Un dato no menor a tener en cuenta es que en el servicio de IM de Google existe una opción OTR. Esta opción no tiene relación con el plugin comentado y no encripta la conversación, sino que [lo único que hace](#) es no grabarla en los logs de la conversaciones en Google Mail, algo que a nadie le consta.

CryptoCat

Si Usted necesita tener una conversación segura en Internet y no dispone de un cliente XMPP ni del plugin OTR, [CryptoCat](#) puede ser de gran utilidad.

CryptoCat no es *la* solución para tener una conversación segura, pero puede resolver de una forma rápida y provisoria el problema. Actualmente se encuentra muy activo su desarrollo y se está implementando soporte para OTR y un cliente para dispositivos móviles.



Cómo anonimizarse al usar Internet

El [proyecto Tor](#) intenta permitir navegar anónimamente por Internet. Esto lo logra utilizando una red de voluntarios que ejecutan servidores para cambiar la ruta por la que un usuario navega por la Red, permitiendo ocultar la información que da cuenta sobre desde dónde se origina la visita. Tor no solamente altera la ruta sino que también encripta múltiples veces los datos, lo que hace extremadamente difícil conocer su origen y su contenido. De todos modos, hay que tener muy claro esto antes de avanzar: el valor agregado de Tor no es proteger el contenido sino anonimizar los datos de quien está navegando.

Originalmente Tor fue creado por el [Laboratorio de Investigación Naval de Estados Unidos](#) para proteger las comunicaciones de gobierno. Actualmente es usado por una comunidad cada vez mayor de hackers, y muy especialmente por activistas, periodistas profesionales de distintas áreas que trabajan con información sensible.

Cómo funciona Tor

Tor crea una suerte de 'túneles' por donde van pasando los datos. En vez de seguir una línea recta entre el usuario y el sitio al que se quiere conectar, Tor crea un camino alternativo. Cada vez que pasa por un túnel, la información se vuelve a encriptar y es enviada hacia el siguiente túnel, hasta alcanzar el punto de salida, donde se conecta al sitio de destino. En todo el trayecto, cada uno de los túneles no conoce

el camino completo. Sólo conoce el túnel anterior de donde vino y hacia dónde tiene que enviarlo a continuación, nada más.

Para crear este camino, Tor utiliza un software especial que le permite conocer cuáles son los servidores disponibles y así seleccionar la ruta a utilizar. Este software permite también que cada diez minutos se pueda volver a cambiar la ruta y de esa forma no poder relacionar las acciones que se venían haciendo con las futuras acciones que realice el usuario.





Un punto a tener en cuenta es que Tor opera desde la máquina del usuario hasta el último servidor antes de llegar a destino. El camino que va desde el último servidor al destino no está protegido y los datos relacionados a ese tráfico son visibles.

Tor no resuelve todos los problemas de anonimidad. Por ejemplo la información que presenta el navegador al conectarse al servicio destino puede ser una fuente para obtener datos del usuario.

Servicios de Tor

Tor no solamente provee un servicio de anonimidad en las comunicaciones. También tiene una serie de servicios adicionales, muy variados y complementarios. En el [sitio Web del proyecto](#) es posible encontrar herramientas incluso para anonimizar el tráfico en televisores inteligentes, por ejemplo. [Un panorama completo y actualizado del ecosistema Tor](#) se presentó en Hamburgo en diciembre del 2012, en el marco del 29th Chaos Communication Congress. Los esenciales:

[Orbot](#), en colaboración [The Guardian Project](#), es un cliente Tor para los teléfonos que funcionan con el sistema operativo Android. Se puede descargar directa y gratuitamente desde Play, la tienda de aplicaciones de Android.

[Tails](#), es un Linux Live, que permite conectarse anónimamente a Tor y no dejar rastros tampoco en el sistema local. Es una distribución Linux diseñada para preservar la privacidad y el anonimato. Está basada en Debian GNU/Linux y puede ser usado como un Live CD o USB sin dejar ningún rastro en el almacenamiento del sistema local, excepto que se indique explícitamente.

[Tor Cloud](#) permite montar un servidor en la nube de Amazon y sumarse a los puentes para acceder a una Internet sin censura. Hay muchos más proyectos, más

técnicos y de infraestructura que se pueden ver en el sitio de Tor.

Tor, también en el teléfono celular

The Guardian Project está realizando una serie de [proyectos relacionados a proteger las comunicaciones realizadas desde dispositivos móviles](#), especialmente para la plataforma Android. Entre ellos se encuentra un cliente Tor, que permite conectarse a la red Tor y tener comunicaciones seguras. [Gibberbot](#), un cliente de mensajería instantánea que se integra con el protocolo OTR para encriptar las comunicaciones. Esta aplicación también es posible descargarla desde la tienda Play en Android.

Cómo construir un túnel privado

Las [Redes Privadas Virtuales \(VPN\)](#) no son nuevas. Hace ya mucho tiempo que existen y nacieron para asegurar las comunicaciones a través de Internet. Son túneles que aíslan conexiones del peligro inherente del tráfico público.

El servicio que ofrece una VPN es el de "asegurar" la comunicación entre dos puntos. Todos los datos que fluyan de un punto al otro de la VPN no podrían, en primera instancia, ser vistos o modificados por cualquier tercero que esté en el medio monitoreando.

Una VPN logra conectar dos puntos sobre Internet enviando todo el tráfico de red a través de túneles y encriptando el contenido. Es de ese modo, aislando y encriptando, que la comunicación establecida queda fuera del alcance de terceros.

Estas conexiones no son físicas, son virtuales. Si dos computadoras están conectadas a Internet, la información puede ser compartida como si estuvieran conectadas físicamente. Es por esto que la forma en que las VPN funcionan es considerada "virtual", porque no hay una conexión física entre los dispositivos.

Es importante notar, que la comunicación es sólo protegida hasta la salida del túnel, que suele ser el proveedor de VPN. Desde este punto hasta el destino, el enlace es como cualquier otro y es susceptible de ser monitoreado. Por ejemplo, si luego de establecer una conexión con el proveedor de VPN, se navega al sitio anonnews.org, la comunicación va a ser encriptada, desde su computadora hasta el proveedor de VPN. De ahí en más la comunicación es como cualquier otra. Esto

implica que cualquier persona que intercepte la comunicación desde ese lado del túnel puede saber todos los datos solicitados y recibidos.

Algo a tener muy en claro es que la VPN "únicamente" asegura o encripta el "canal" por donde se produce la comunicación. Con esto queremos dejar en claro que cualquier dato que se introduzca por el canal o que se saque por el otro extremo, si no se toman los recaudos necesarios, es susceptible de ser interceptado.

Existen actualmente muchos servicios de VPN que por un abono mensual o anual ofrecen la solución de un canal seguro a usuarios finales. El primer punto a evaluar de estos servicios es dónde alojan sus servidores y bajo qué jurisdicción legal se rigen. Ya que ante el reclamo de los datos de una fuente, el proveedor del servicio de VPN puede informar desde qué IP se produjo la conexión.

Servicios de VPN

Los servicios gratuitos de VPN suelen ser promocionados con publicidad o limitados en el ancho de banda que permiten usar. Los servicios pagos no suelen tener estas limitaciones. Algunos servicios que podemos nombrar son:

Hotspot Shield, <https://hotspotshield.com>

FreeVPN, <http://www.thefreevpn.com>

CyberGhost, <http://cyberghostvpn.com>

Vpnod, <http://www.vpnod.com>

Anonymizer, <https://www.anonymizer.com/>

Xerobank, <https://xerobank.com/>

HotSpot VPN, <http://www.hotspotvpn.com/>

RiseuoVPN, <https://help.riseup.net/es/vpn>

Una alternativa a los servicios arancelados es configurar su propio servicio de VPN. Esto requiere un más alto nivel técnico, pero el servicio luego será gratis. La naturaleza privada de esta configuración también lo hace menos vulnerable a que sea bloqueado. Uno de los softwares más utilizados es [OpenVPN](#).

Estándares VPN y encriptación

Hay diferentes estándares para configurar una red VPN, incluyendo [IPSec](#), [SSL/TLS](#) y [PPTP](#), que varían en términos de complejidad y nivel de seguridad.

PPTP es conocido por tener un sistema de encriptación débil, pero puede ser útil para la acción de sortear un bloqueo de Internet. Es simple de configurar y está disponible para la mayoría de los sistemas operativos. SSL/TLS son sistemas relativamente simples de configurar y proveen un sólido nivel de seguridad.

IPSec opera a nivel de red y es responsable de la transferencia de paquetes en Internet, mientras los otros se ejecutan a nivel de aplicación. Esto hace a IPSec más flexible pero también más difícil de configurar.

Cómo tener una privacidad "bastante buena"

[Pretty Good Privacy \(PGP\)](#) es un software para encriptar y desencriptar información.

PGP utiliza un método de encriptación denominado de clave pública o asimétrico. Consiste en la utilización de dos claves que funcionan en conjunto. Una, la privada, es tenida a resguardo por el propietario y jamás divulgada. La otra, la pública, puede ser distribuida libremente por cualquier medio.

Su funcionamiento es simple: Si A debe enviar un mensaje a B, A toma la clave pública de B para encriptar el mensaje que enviará. El único que puede conocer el mensaje es B, que para desencriptarlo debe usar su clave privada.

La única forma de desencriptar ese mensaje es utilizando la clave privada, cuyo único poseedor es el destinatario. Ninguna persona que posea la clave pública del destinatario podrá desencriptar el mensaje. De esta manera se puede enviar un mensaje encriptado por una red pública como Internet sin temor a que su contenido pueda ser visto.

Cada sistema operativo tiene su propia distribución de PGP . Y en cada caso, además, varía la forma de instalación.

Linux: [GnuPG](#). Cada distribución de Linux tiene su propio manejador de paquetes. Se deberá buscar por GnuPG e instalarlo.

OS X: [GpgTools](#) es la implementación para Mac que ofrece varias herramientas además de PGP, incluyendo integración con el administrador de claves de OS X.

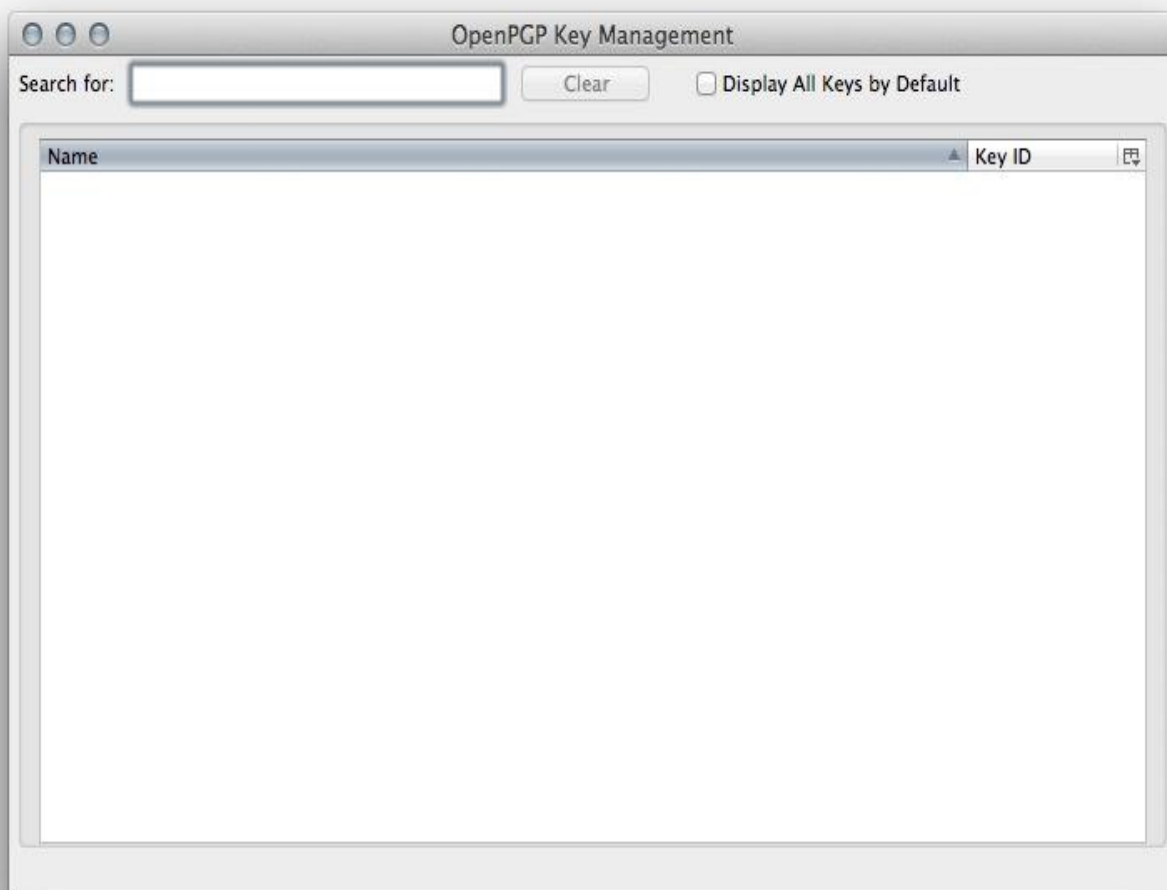
Windows: [Gpg4Win](#) es la implementación para Windows que incluye integración con Outlook e Internet Explorer.

Una de las formas más simple de utilizar PGP para encriptar los correos es utilizando el [plugin Enigmail](#) de [Thunderbird](#) tanto en Linux, Mac o Windows. En Linux los clientes de correo nativos como Evolution o KMail ya vienen con soporte nativo para PGP. En Mac, la herramienta GpgTools incluye varias utilidades, entre ellas una para integrarla con la aplicación Mail, el software nativo de Apple para la gestión de correos electrónicos.

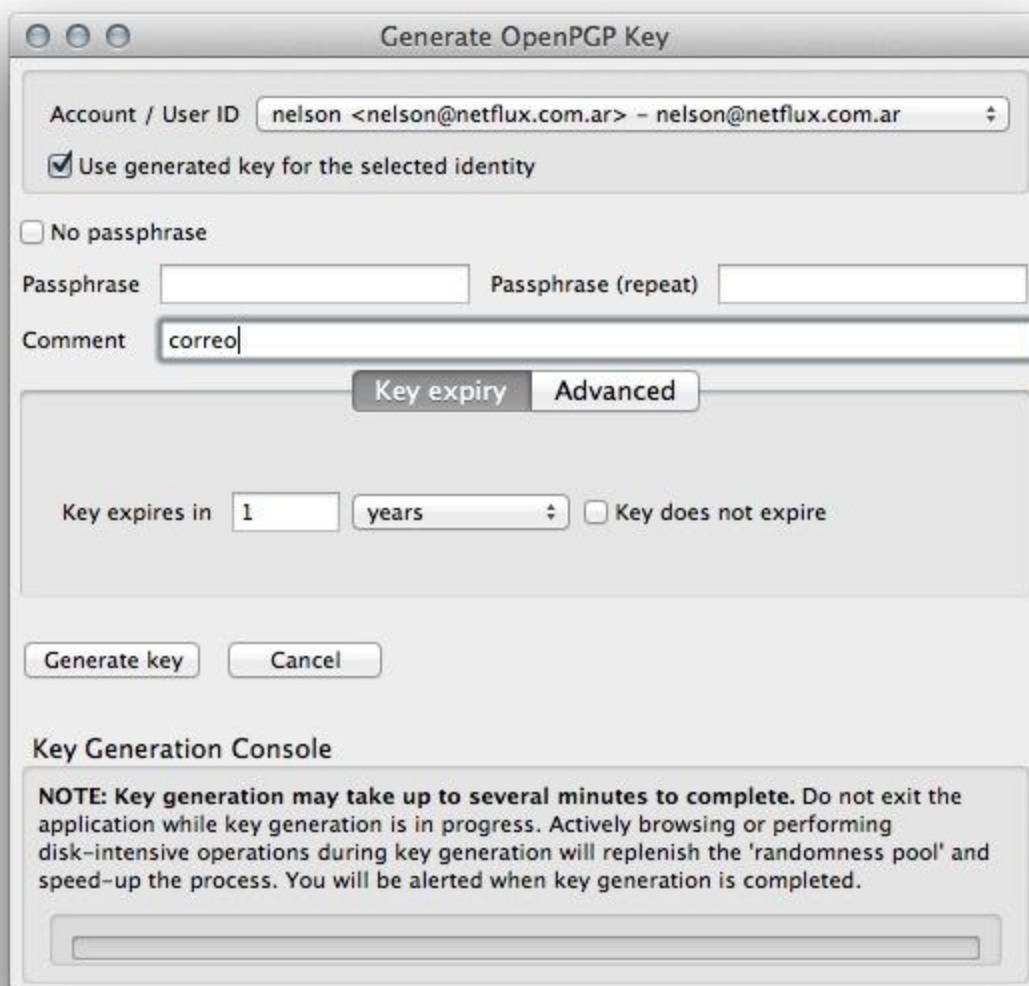
Generando la primera clave PGP

En los siguientes ejemplos se utilizará la aplicación [Thunderbird](#) con el plugin Enigmail para generar la primera clave PGP y encriptar un correo. Se decidió de esta manera ya que es un programa multiplataforma que funciona en todos los sistemas operativos de la misma manera. Los conceptos que se verán se pueden aplicar luego a cualquiera de los otros clientes de correo.

Luego de haber instalado PGP, Thunderbird y el plugin Enigmail, al abrir Thunderbird Usted encontrará un menú nuevo que se llama OpenPGP. Allí verá la opción Key Management. Al seleccionarla se abrirá una ventana que le permitirá gestionar las claves PGP que posea:



Quando Usted abra esa ventana se le presentará un nuevo menú que tiene la opción Generate y un submenú New Key Pair, que una vez seleccionado le ofrecerá las siguientes opciones:



Aquí podrá seleccionar la cuenta de correo para la cual se va a generar el par de claves, una clave de seguridad que se le será solicitada cada vez que la use, un campo de comentario y la fecha de expiración de la clave. Un valor razonable para la fecha de expiración es de 1 año y nunca debería ser mayor a 2 años. Como es posible tener y usar varias claves PGP por cada cuenta de correo, es bueno utilizar el campo comentario para

especificar el uso que se pretende dar a esa clave, así al momento de seleccionarla es más simple:



En las opciones avanzadas (Advanced) se puede configurar el tipo y tamaño de la clave.

Para los estándares actuales, el tamaño de clave no debería ser menor a 4096 y el tipo de clave debe ser [RSA](#).

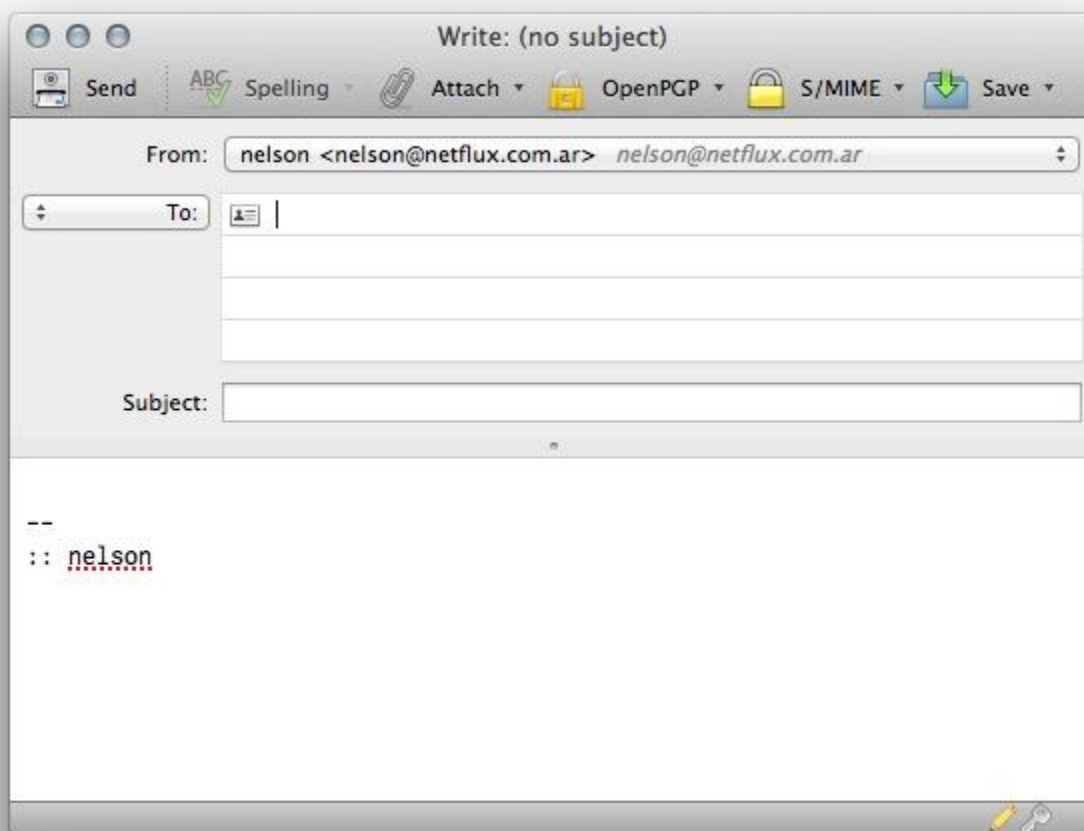
Una vez elegidas estas opciones, Usted puede oprimir el botón de Generate Key para comenzar el proceso de la generación de la clave. Este proceso es lento y verá que la barra de progreso avanzar despacio. Tranquilo. Esto es así porque se están tomando múltiples patrones al azar de procesos que están en segundo plano, para generar la suficiente aleatoriedad de tal modo de que la clave sea segura:



Terminado el proceso se le va a preguntar si desea generar un certificado de revocación. Este certificado va a ser utilizado únicamente en el caso de que pierda

su clave privada, la contraseña para utilizarla o en caso de que la clave privada haya sido comprometida, es decir, haya salido de su propiedad.

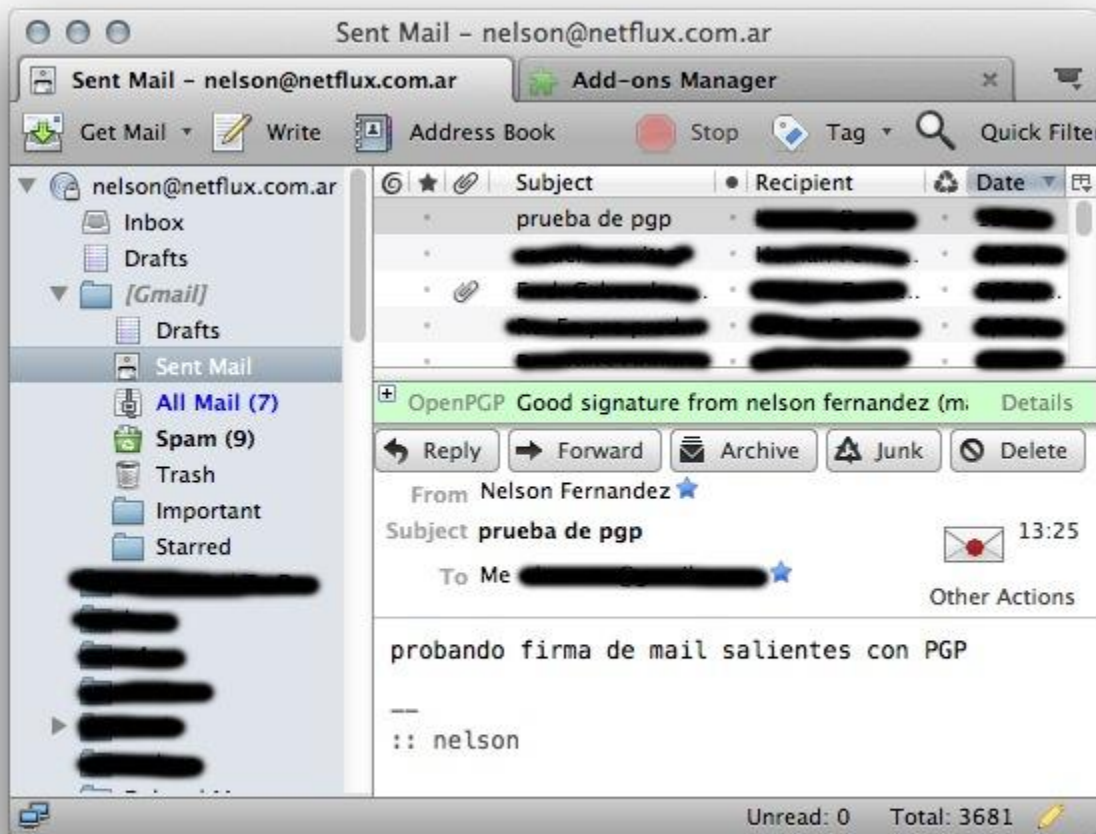
Una buena práctica es mover este certificado de revocación a un cd-rom o a un pendrive y dejarlo a buen resguardo, y por supuesto, con acceso bajo clave. Ya que en caso de que alguien tuviera acceso a este certificado, podría invalidar su clave privada:



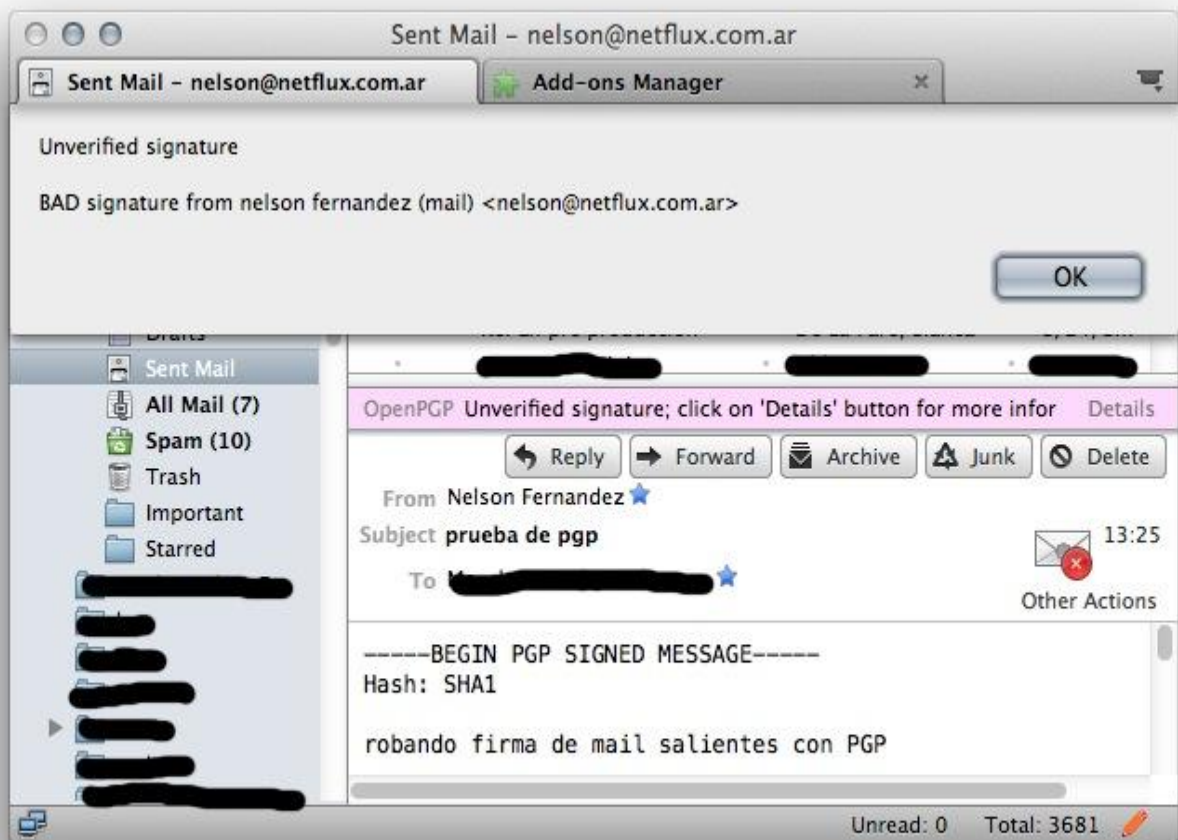
Muy bien, ahora cuando Usted crea un email en Thunderbird obtendrá un nuevo icono etiquetado como

OpenPGP, que tiene las opciones, Sign Message y Encrypt Message (Firmar y Encriptar Mensaje) que le permitirán firmar los mensajes, para que el destinatario pueda verificar su autoría y/o encriptar el mensaje. De esta manera Usted puede enviar un mensaje de forma segura y que sólo sea visto por el destinatario y por nadie más.

De ahora en adelante, cada vez que necesite acceder a la clave privada, se le va a solicitar la contraseña que se pidió cuando la generó, y si el mensaje será validado, y se mostrará una línea verde en la cabecera:



En caso de que la firma no pueda ser verificada, la barra será de color rosa. Esto implica que el mensaje fue modificado de alguna forma y no puede ser verificado:



Cómo asegurar su teléfono

Los dispositivos móviles son usados cada vez más para las tareas más diversas: desde enviar correos electrónicos, establecer conversaciones de mensajería instantánea y tomar fotografías, hasta funciones bastante más críticas, como acceder a servicios de home banking, o usar la VPN de la empresa. Por esta razón, y por la cantidad de información que cuenta sobre Usted, su teléfono celular se puede transformar en un bien preciado, es decir, en un dispositivo que debe proteger bajo "siete llaves".

Asegurar tanto las conversaciones como el mismo acceso al dispositivo debe ser hoy un requisito indispensable. Un periodista tomando fotos y enviando reportes de los hechos que cubre puede ser algo normal. Pero si esos hechos se producen en un ambiente hostil donde las libertades de prensa y/o individuales son escasas, y encontrar ese material puede poner al periodista en una situación comprometida, toda acción que proteja o impida el acceso a esa información debe ser tomada en cuenta.

Por todo eso, la primer medida y más básica debe ser tener siempre protegido el acceso al teléfono por contraseña, o por alguno de los métodos que provea el teléfono. Esa simple medida ya eleva la seguridad de los datos. En ese caso, accederlos no será imposible, pero los recursos técnicos necesarios para lograrlo derán ser mucho mayores.

Otras sugerencias simples que mejoran la seguridad del dispositivo:

- Activar el ingreso por contraseña cuando no se usa el móvil por un tiempo determinado.
- Activar que los datos sean borrados luego de una cantidad N de intentos errados al ingresar la contraseña para acceder al dispositivo.
- Mantener todo el software que se utilice actualizado.

Otras medidas que Usted debe tomar son aquellas relacionadas a las comunicaciones. Y en este sentido el trabajo que está realizando [The Guardian Project](#) es notable. Están creando un conjunto de herramientas que permiten asegurar todas las comunicaciones del teléfono. Desde la navegación por internet, hasta el borrado de datos sensibles del teléfono en caso de necesidad.

Esta es una breve enumeración de los proyectos que están llevando a cabo y que le sugerimos se haga el tiempo de probar en su teléfono. Son gratis, fáciles de instalar y nada difíciles de usar:

[Orbot](#)

Implementación del protocolo Tor. Esto permite navegar anónimamente desde el teléfono y acceder a sitios que pueden estar bloqueados localmente.

[Orweb](#)

Navegador de Internet con una mejora en seguridad por defecto. Por ejemplo: no almacena el historial de navegación, cookies, deshabilita flash y evita ciertos patrones de análisis de Red.

[Gibberbot](#)

Es un cliente de IM basado en XMPP que implementa el protocolo OTR para tener conversaciones seguras.

ObscuraCam

Es una cámara de fotos que puede oscurecer, encriptar o destruir píxeles de una imagen. También se está trabajando para tener este soporte en la gestión de videos.

ProxyMobile

Es una extensión para la versión móvil de Firefox, que le permite navegar a través de un proxy, logrando que se pueda usar con la red Tor.

Panic! ("InTheClear")

Una aplicación muy sencilla y poderosa a la vez: un botón rojo que cuando Usted lo presione, eliminará toda la información sensible del dispositivo. Sin vuelta atrás.

K-9 y APG

Es un cliente de correo que tiene soporte para PGP. Le permite firmar y encriptar los correos.

TextSecure

Es un cliente para gestionar mensajes SMS, que permite almacenarlos de forma segura. Si la otra persona que los recibe también usa este software, permite encriptar todo ese intercambio de textos.

CSipSimple

Es un cliente SIP (cliente [VoIP](#)) que provee encriptación de voz. No usa la red de voz para las llamadas, sino que las realiza sobre Internet.

Cómo encriptar un disco

La mejor herramienta de código abierto para encriptar un disco rígido es sin lugar a dudas [TrueCrypt](#). Es multiplataforma (Linux, Mac, Windows) y de muy simple uso. Puede generar un archivo encriptado y tratarlo como si fuera un disco. También puede encriptar directamente una partición o disco externo o USB.

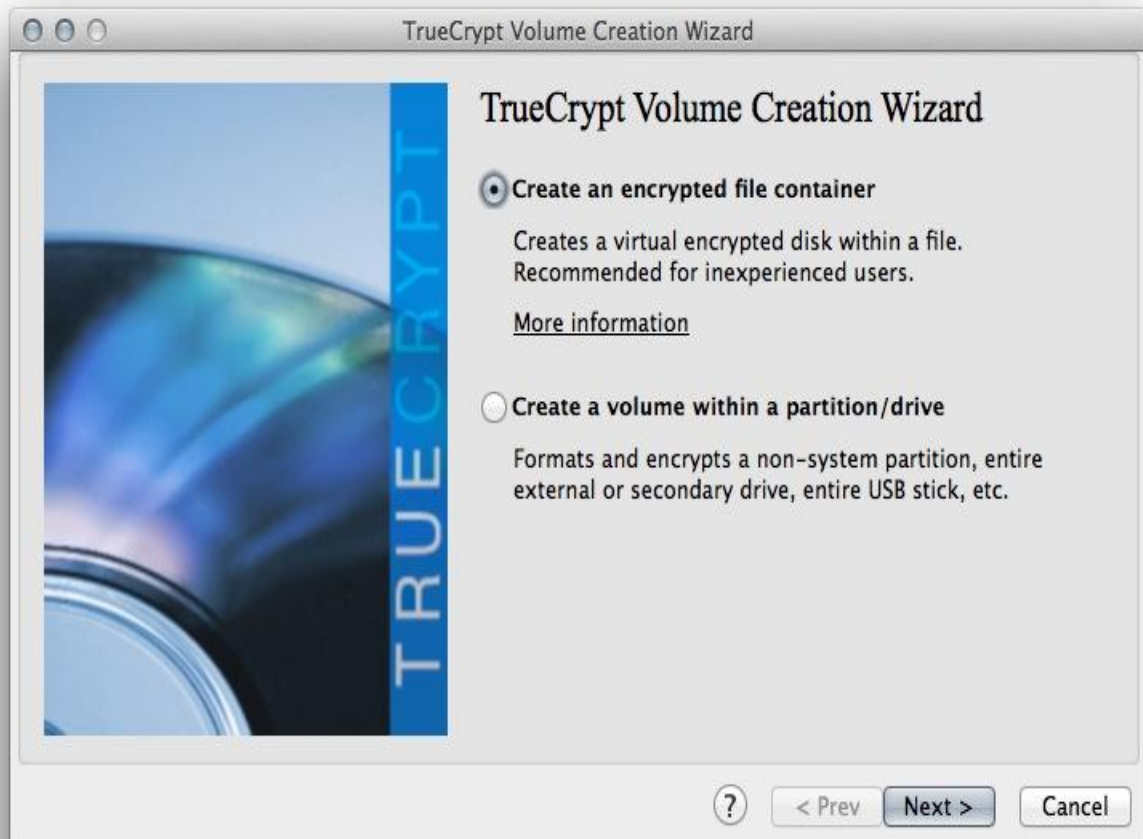
TrueCrypt tiene una característica muy interesante: la posibilidad de crear Particiones Ocultas (Hidden Volume). Esta característica permite ocultar la existencia de un espacio donde se guardan archivos, dentro del propio disco encriptado. En ese caso, si alguien tuviese acceso a su computadora o a un disco de su propiedad en el que Usted guarda archivos sensibles, no podría tener acceso a las carpetas que Usted haya definido como inaccesibles.

Un ejemplo extremo pero no por eso improbable es la situación que muchos periodistas de todo el mundo enfrentan a diario. Si Usted se ve forzado o lo extorsionan para revelar las claves de acceso a su dispositivo o incluso al disco encriptado, nadie podrá ver aquella información que es para Usted realmente valiosa. Cuando un tercero tenga acceso no podrá ver la partición oculta, ni sabrá de su existencia.

Al ejecutar TrueCrypt se le presentará una ventana con los "Slots" disponibles para crear particiones o discos encriptados.

Con el botón Create Volume comienza el proceso de creación de una partición. Se le consultará si desea

crear un archivo contenedor o encriptar un disco o partición:

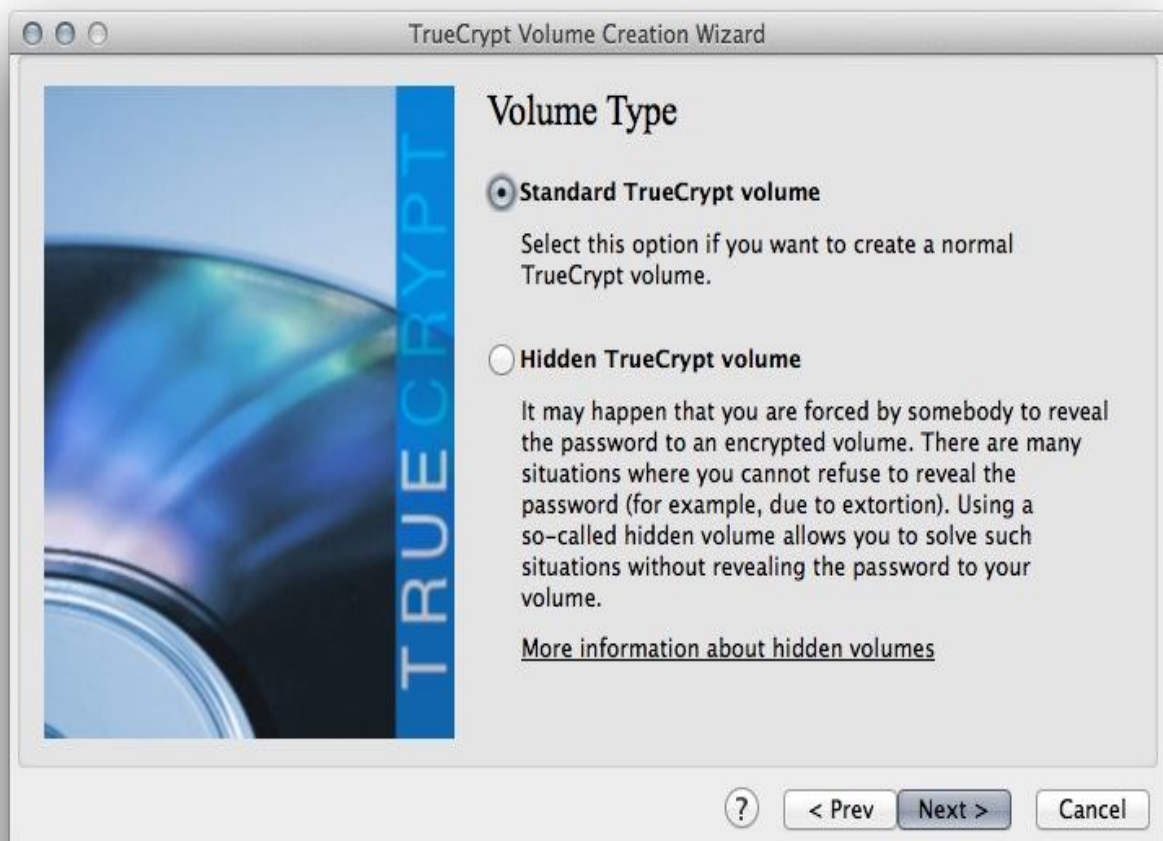


La opción de un archivo contenedor crea un archivo que puede alojarse en el disco rígido o USB drive, el cual físicamente es como un archivo común, y puede ser copiado o borrado normalmente como cualquier otro.

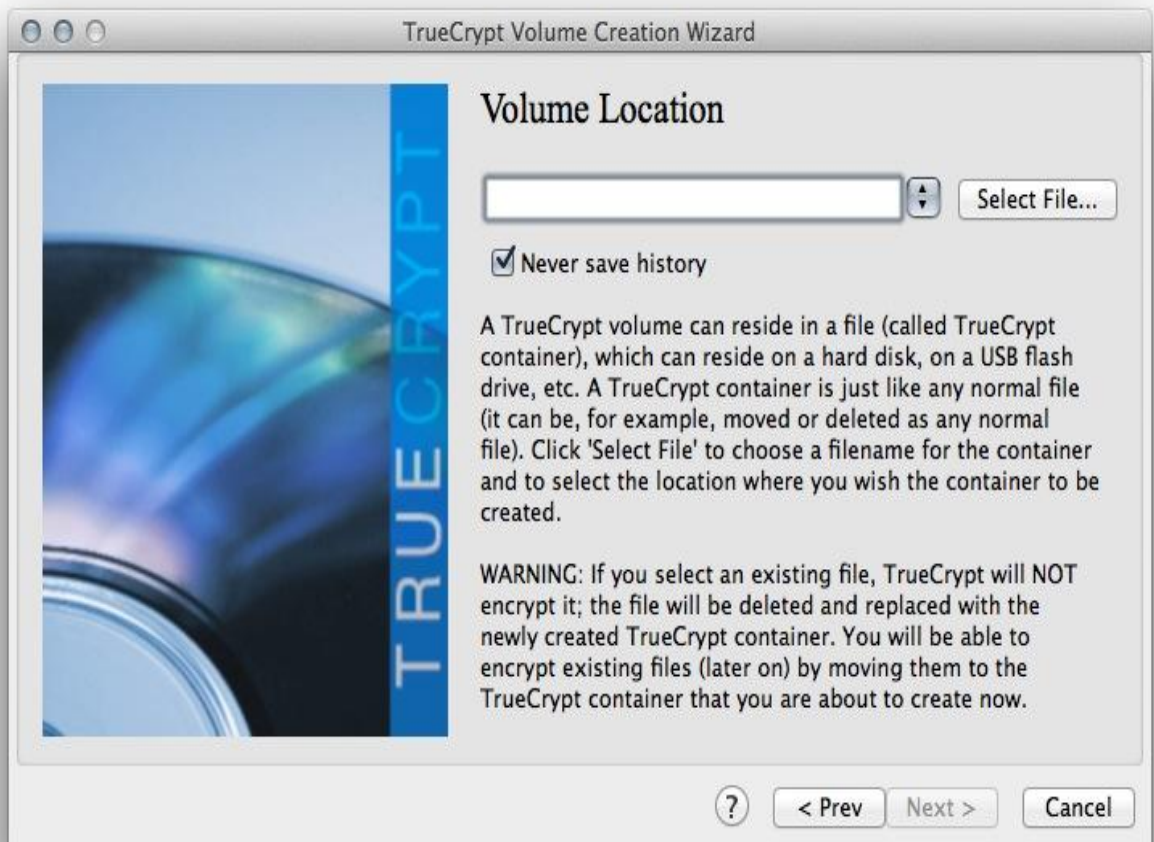
Seleccionando la opción de crear un archivo contenedor (Create an encrypted file container), se deberá decidir si la partición será una de tipo normal (Standard) o una oculta (Hidden).

Las particiones ocultas se crean sobre una partición ya existente y es, precisamente, el tipo de partición que mencionábamos antes, las cuales sólo pueden ser accedidas si se sabe de su existencia y se ingresa la clave correcta. En caso contrario sólo se muestra su partición contenedora y la oculta será indetectable, invisible.

Luego de crear la partición normal, creará la oculta:

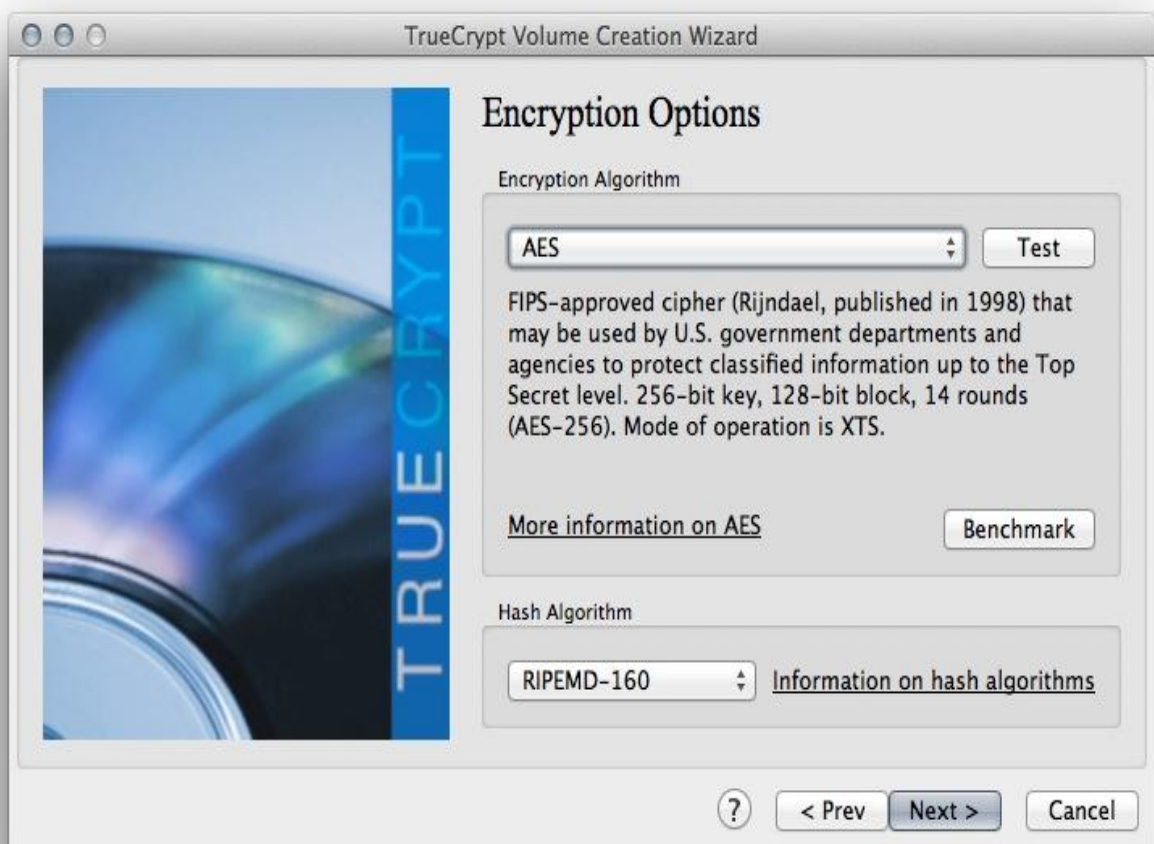


En este punto debe elegir qué nombre darle al archivo y dónde será creado:



Ahora tendrá que seleccionar dos parámetros muy técnicos, como son el algoritmo de encriptación y el de digesto. Por defecto el algoritmo de encriptación es [AES](#), que es un estandar desde 1998 y no hay evidencia de que haya sido vulnerado. Las otras opciones que aparecen son los otros finalistas de esa selección (Twofish y Serpent) y modalidades de uso combinando los algoritmos.

Salvo que sepa exactamente lo que está haciendo, será prudente que deje los valores que vienen por defecto:



El siguiente paso es seleccionar la capacidad de este archivo. Debe tener en cuenta que una vez creado no se podrá modificar su tamaño. Es clave que preste atención entonces a qué tipo de archivos guardará dentro del disco encriptado.



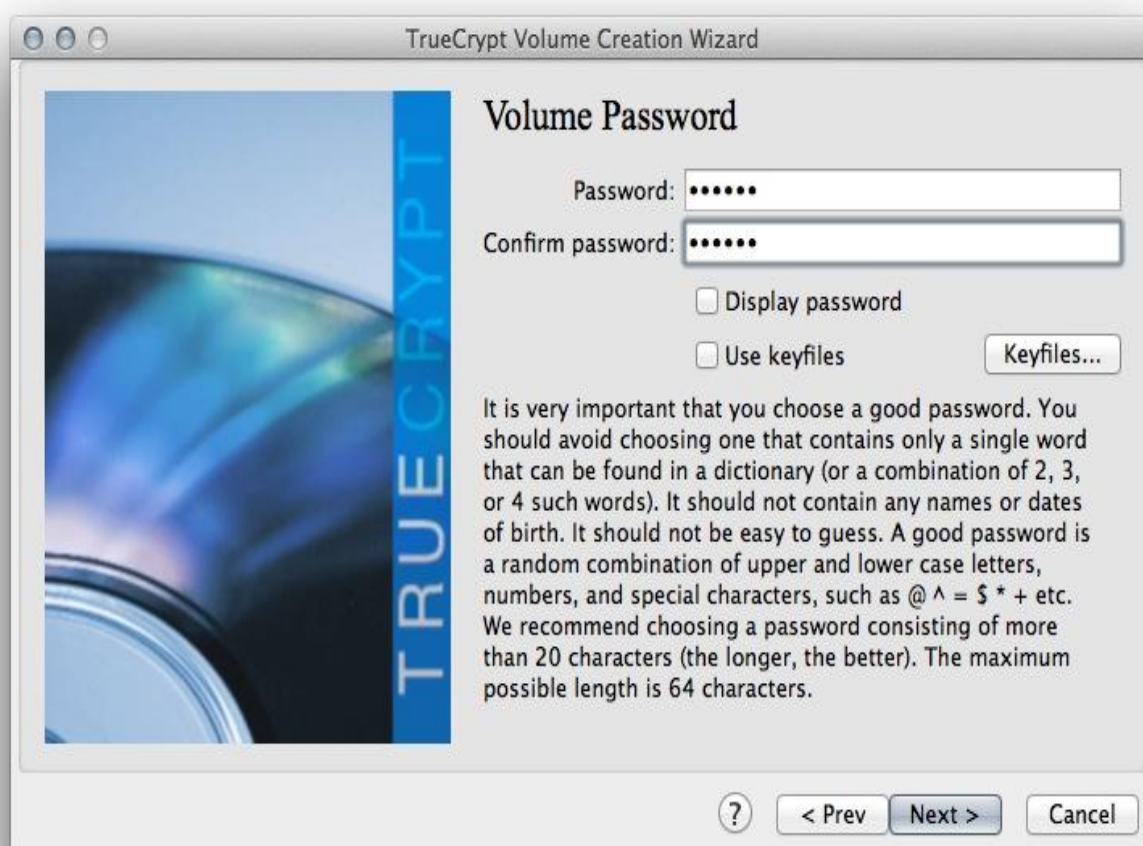
Y finalmente se le solicitará seleccionar la clave para proteger el disco.

Una opción extra que se presentará es el uso de 'keyfiles'. Estos archivos, que pueden ser de cualquier tipo, como un mp3, .avi, .zip, etc., y cualquier cantidad, permiten agregar un paso más para tener acceso y así seguir fortaleciendo la seguridad de sus contenidos.

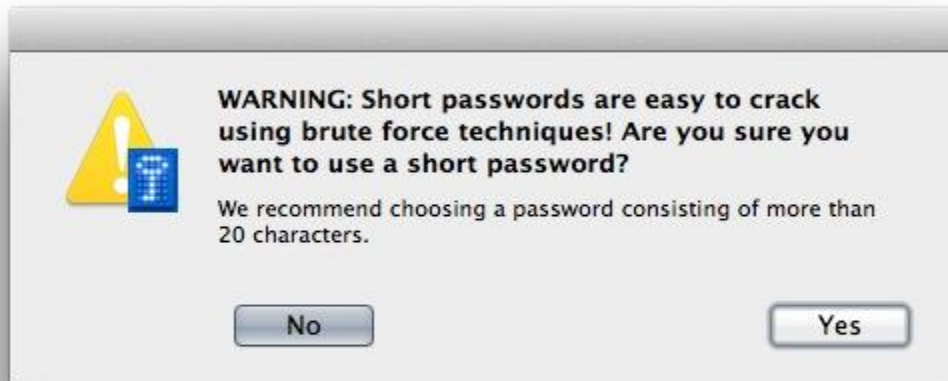
Lo ideal en caso de utilizar keyfiles, es accederlos mediante una Smartcard o un Token de seguridad. De esta manera Usted agrega un segundo

factor de autenticación que no se basa en algo que “sabe”, sino en algo que “tiene”. En el caso de que pierda el archivo encriptado y que alguien conozca la clave de seguridad para accederlo, si no se tienen los keyfiles, no se podrá acceder.

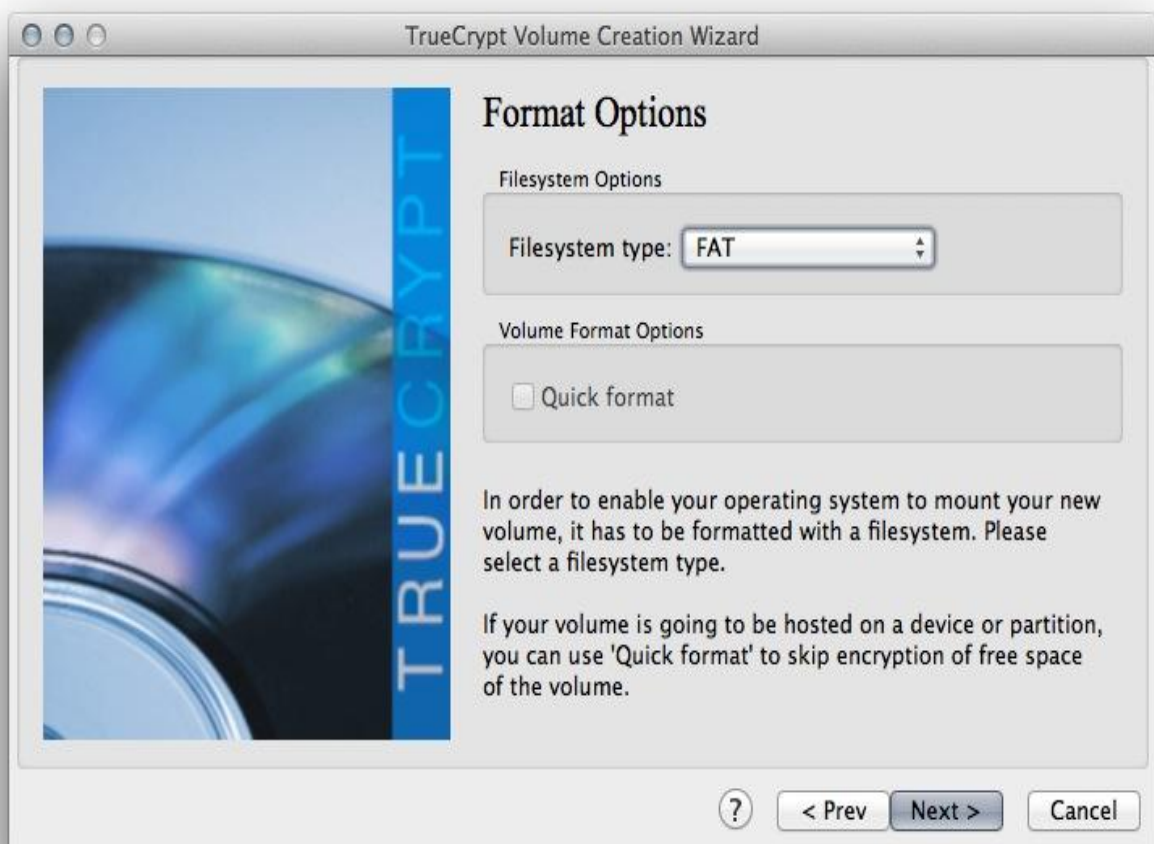
Así mismo se pueden utilizar los keyfiles para armar esquemas de acceso en los que se requiera la presencia física de dos o tres personas para abrir un archivo encriptado:



Si elige una clave poco segura, se le pedirá confirmar para continuar:



Y finalmente se le preguntará qué tipo de formato le dará al disco encriptado. Lo ideal quizás sea utilizar FAT, para tener un formato que se pueda utilizar desde distintas computadoras y sistemas operativos:



Una vez seleccionado, se verá una pantalla donde se visualizará el proceso de creación de este disco encriptado.

En la etiqueta 'Random Pool' verá la generación de distintos números, y cuando mueva el ratón sobre la ventana, esta generación será más rápida. Esto se debe a que para generar estos números al azar se están tomando distintos parámetros del sistema y uno de ellos es la posición del mouse.

Deberá mover el ratón sobre la ventana a intervalos irregulares y usando distintos patrones durante dos o

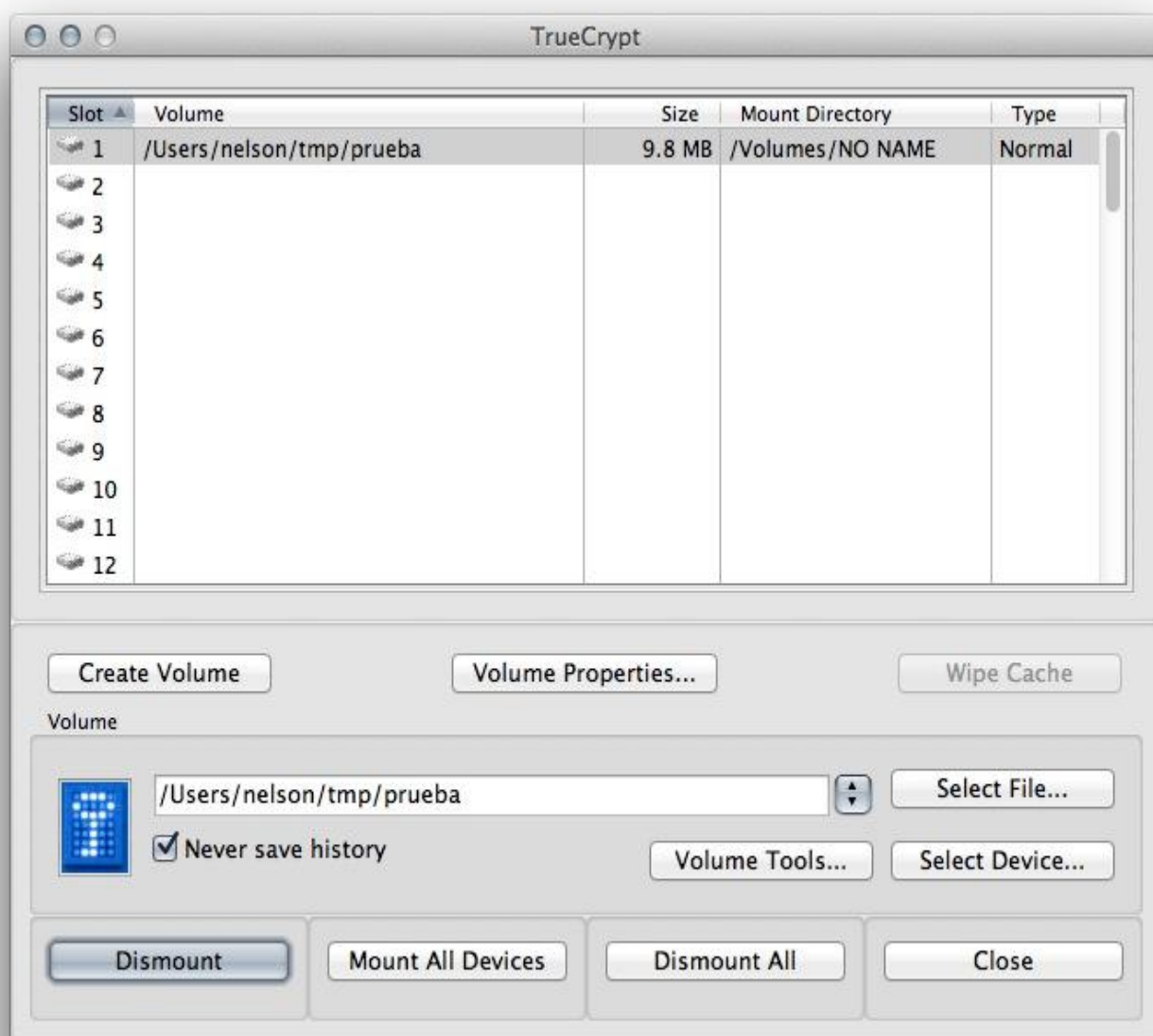
tres minutos, para generar la suficiente cantidad de números al azar.

Luego podrá oprimir el botón Format y comenzará el proceso de creación:



Después de haber creado el archivo encriptado, volverá a la ventana original. Aquí, oprimiendo el botón Select File, elegirá el archivo recién creado y luego oprimirá el botón Mount donde se le solicitará la clave para accederlo.

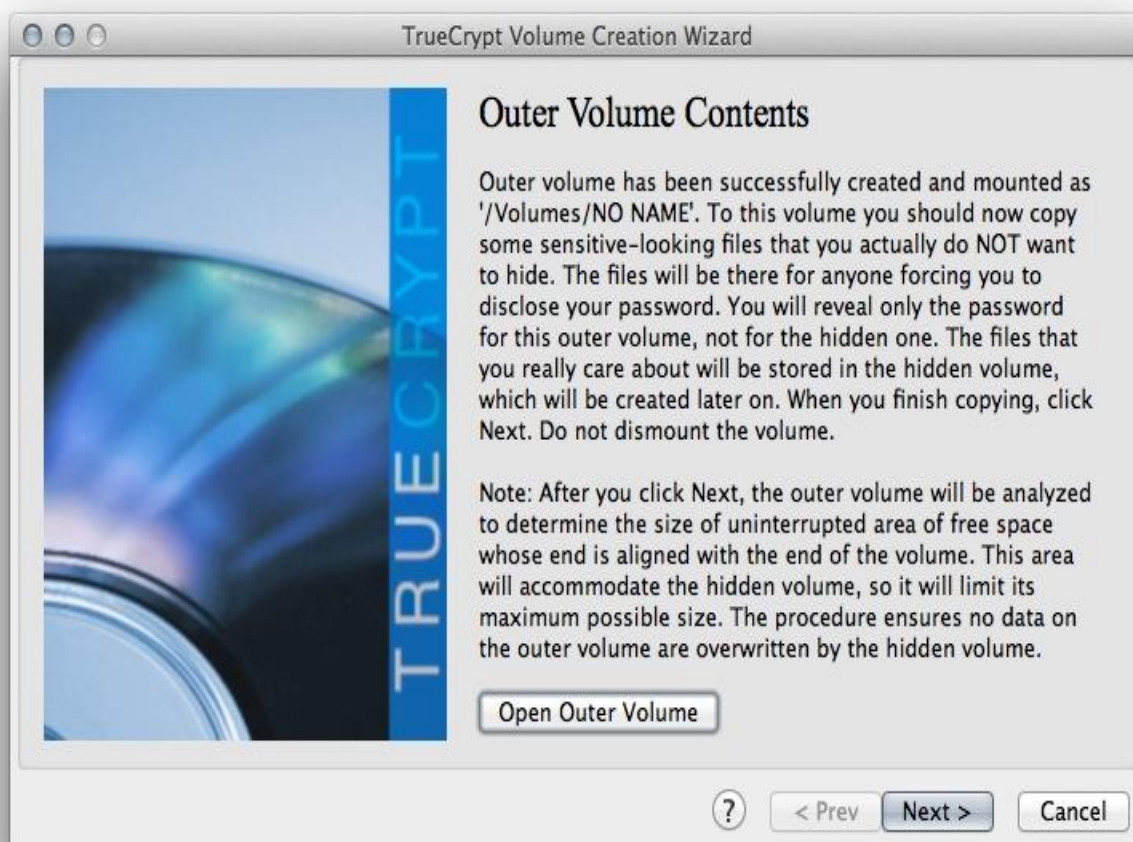
Dependiendo del sistema operativo, se le solicitará o no la clave de administrador para montar el disco encriptado:



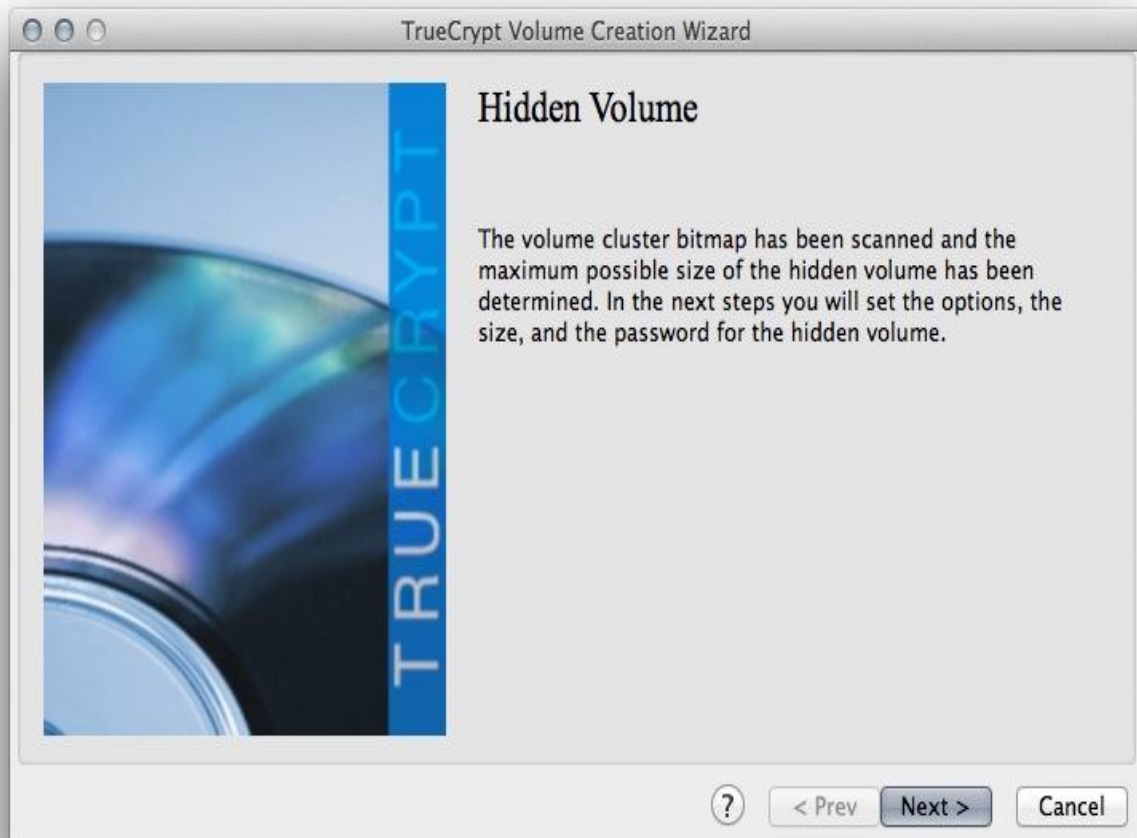
Particiones Ocultas

La creación de una partición oculta es prácticamente igual al proceso descrito anteriormente. La única diferencia es que al momento de ser solicitada la clave de acceso, primero deberá poner una clave Exterior (Outer Volume Password). Esta clave es aquella que permitirá acceder al disco encriptado.

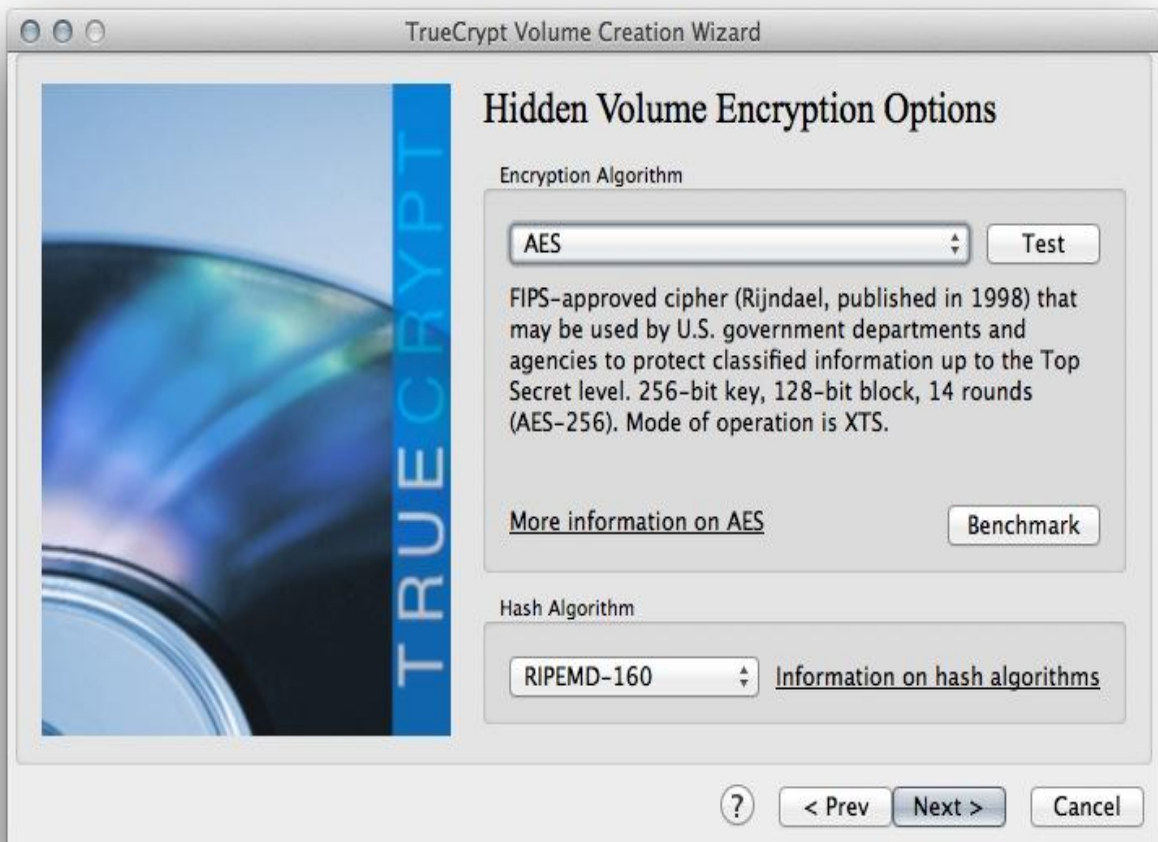
Una vez creada y formateada esta partición, se le permitirá abrirla y agregar algunos archivos que eventualmente puedan ser expuestos:



Avanzando, comienza el proceso de creación de la partición oculta en el espacio restante de la primera partición. Allí seleccionará Usted los parámetros de encriptación y la cantidad de espacio de esta partición oculta:



También la clave para acceder a este volumen encriptado (Hidden Volume Password):



Luego pasará por las pantallas del proceso de creación, pero esta vez será para crear el volumen oculto.

Una vez terminado este proceso Usted podrá montar el volumen y, dependiendo de la clave que utilice, verá el contenido del volumen exterior o del volumen oculto:



The hidden TrueCrypt volume has been successfully created and is ready for use. If all the instructions have been followed and if the precautions and requirements listed in the section "Security Requirements and Precautions Pertaining to Hidden Volumes" in the TrueCrypt User's Guide are followed, it should be impossible to prove that the hidden volume exists, even when the outer volume is mounted.

WARNING: IF YOU DO NOT PROTECT THE HIDDEN VOLUME (FOR INFORMATION ON HOW TO DO SO, REFER TO THE SECTION "PROTECTION OF HIDDEN VOLUMES AGAINST DAMAGE" IN THE TRUECRYPT USER'S GUIDE), DO NOT WRITE TO THE OUTER VOLUME. OTHERWISE, YOU MAY OVERWRITE AND DAMAGE THE HIDDEN VOLUME!

OK

Nos vemos en el café de la esquina

Si Usted necesita tener una conversación virtual privada, salga de ahí. La mejor idea es tomar la laptop e ir al café de la esquina. Pida un café y conéctese a la Red. Una Red distinta a la suya, a la de su casa o a la de su lugar de trabajo, que no puede ser asociada a Usted ni a datos relacionados con su persona, es una conexión en la cual nadie lo conoce. Pero no está a salvo.

El mayor problema es que ahora las miradas son invisibles. No vamos a poder identificar quién está observando, ni desde dónde. Y ahí está el gran truco, casi como describen en la película *Los Sospechosos de Siempre* a Keyser Söze: "El gran truco del diablo fue hacer creer que no existía".

Entonces la forma de poder protegerse es tratando de entender con qué herramientas lo pueden espiar, cómo funcionan y con esa información y conocimiento minimizar los riesgos.

Desde una red pública, y esto se aplica tanto a wifi como a redes de celulares (3g, lte, etc.), es muy simple de poder acceder a toda la comunicación ya que el transporte es el aire.

Cuando se conecta a cualquier servicio web (home banking, correo, Facebook, etc.) se crea una sesión entre su máquina y el servicio. A esta sesión se le asigna un número para identificarla y se la guarda en el navegador en la forma de una cookie. De ahora en más, cada vez que hace una interacción con el servicio, es

decir cada vez interactúa en el sitio haciendo click en un link, debe presentar esa cookie que tienen su identificador para seguir usando el servicio normalmente. Caso contrario, el servicio no lo podrá identificar y le pedirá registrarse nuevamente.

La primera forma de que los puedan espiar es intentando robar esa cookie. Accediendo a ella, pueden hacerse pasar por Usted y acceder al servicio. No le están robando el usuario y la clave del servicio, pero sin embargo pueden acceder a su cuenta.

El robo de cookies de sesión se denomina asalto de sesión ([session hijacking](#)) y éstas son algunas formas de lograrlo:

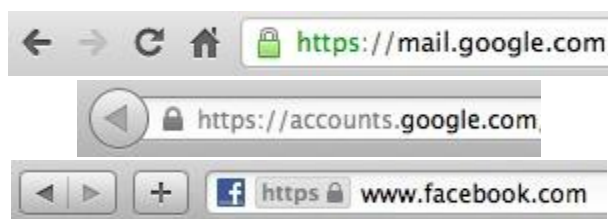
- Fijación de sesión ([session fixation](#)). Este tipo de ataque trata de imponerle un identificador de sesión. Es utilizado muchas veces enviando un mail con un link al servicio. La forma más simple de protegerse: nunca haga click en un link que le envía por correo un desconocido. Y si es una persona conocida, asegúrese que no es un tercero haciéndose pasar por esa persona. Vea desde dónde le envían el correo y escriba la url del sitio en el navegador: sólo la dirección del sitio, por ejemplo: `www.banco.com`, y no la url completa que recibió.

- Ejecución fuera del sitio ([cross-site scripting](#)). Este proceso es un poco más complejo técnicamente, pero es uno de las más utilizados. Lo que trata de lograr es ejecutar código en el navegador haciéndose pasar como si hubiera sido provisto por el sitio al que está accediendo. De esa forma pueden obtener la cookie que tiene su identificador de sesión. Nuevamente la forma de inyectar este código es que primero visite una url

dada. Así las cosas, la mejor forma de evitarlo es no seguir directamente url que le fue enviada sino escribirla en el browser.

- Y la más compleja técnicamente es llamada Session Sidejacking y es realizada monitoreando el tráfico que genera el usuario. En base a este monitoreo se puede obtener información de la sesión y de ahí obtener el usuario y clave, o el identificador de sesión. Este monitoreo es mucho más simple cuando Usted se encuentra conectado a una red compartida, como en el caso del un wifi en un lugar público.

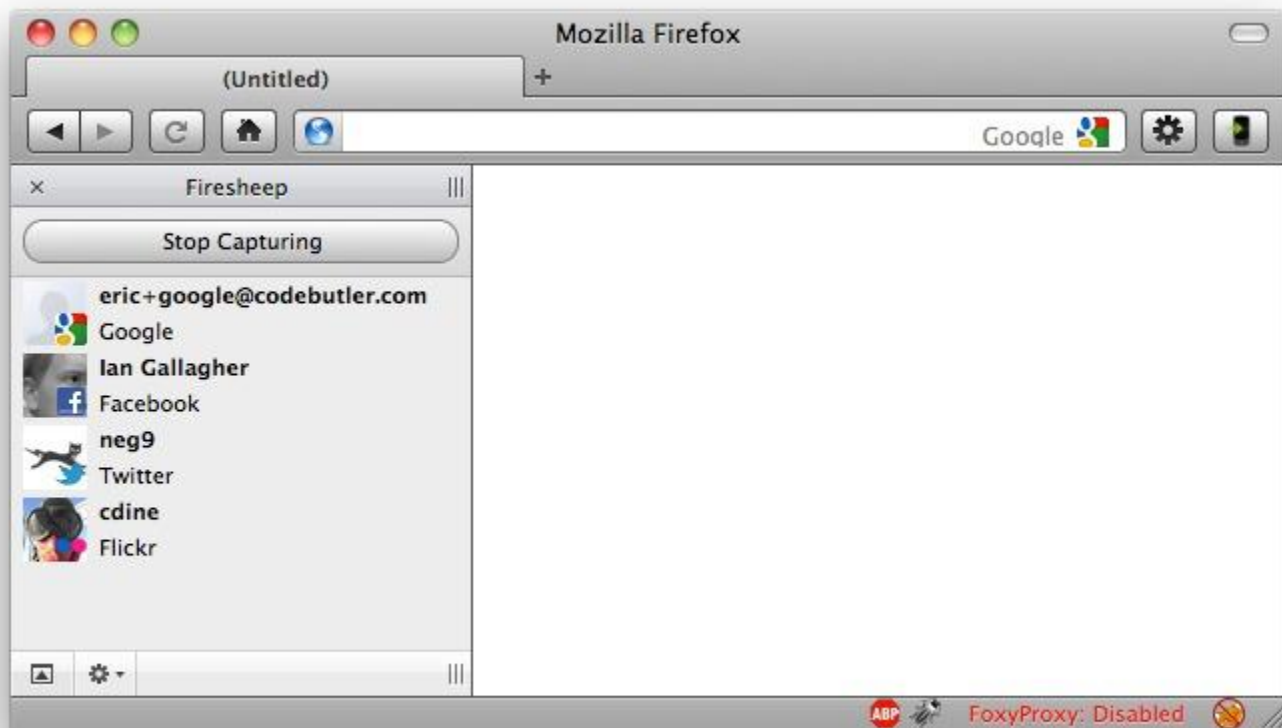
La única forma de protegerse de este tipo de ataques es asegurándose de utilizar siempre una conexión segura denominada HTTPS. Este tipo de conexión es fácilmente identificable porque cambia el ícono en la barra del navegador:



La conexión HTTPS no solo debe existir durante el proceso de autenticación, donde se ingresa usuario y clave, sino durante toda la sesión. Caso contrario, como ya vimos, no hace falta el usuario y clave, sino con el identificador de sesión es posible que un tercero ingrese al servicio haciéndose pasar por Usted.

A modo ilustrativo podemos ver como funciona la aplicación [Firesheep](#): permite analizar el tráfico de

una red pública y obtener los identificadores de sesión:



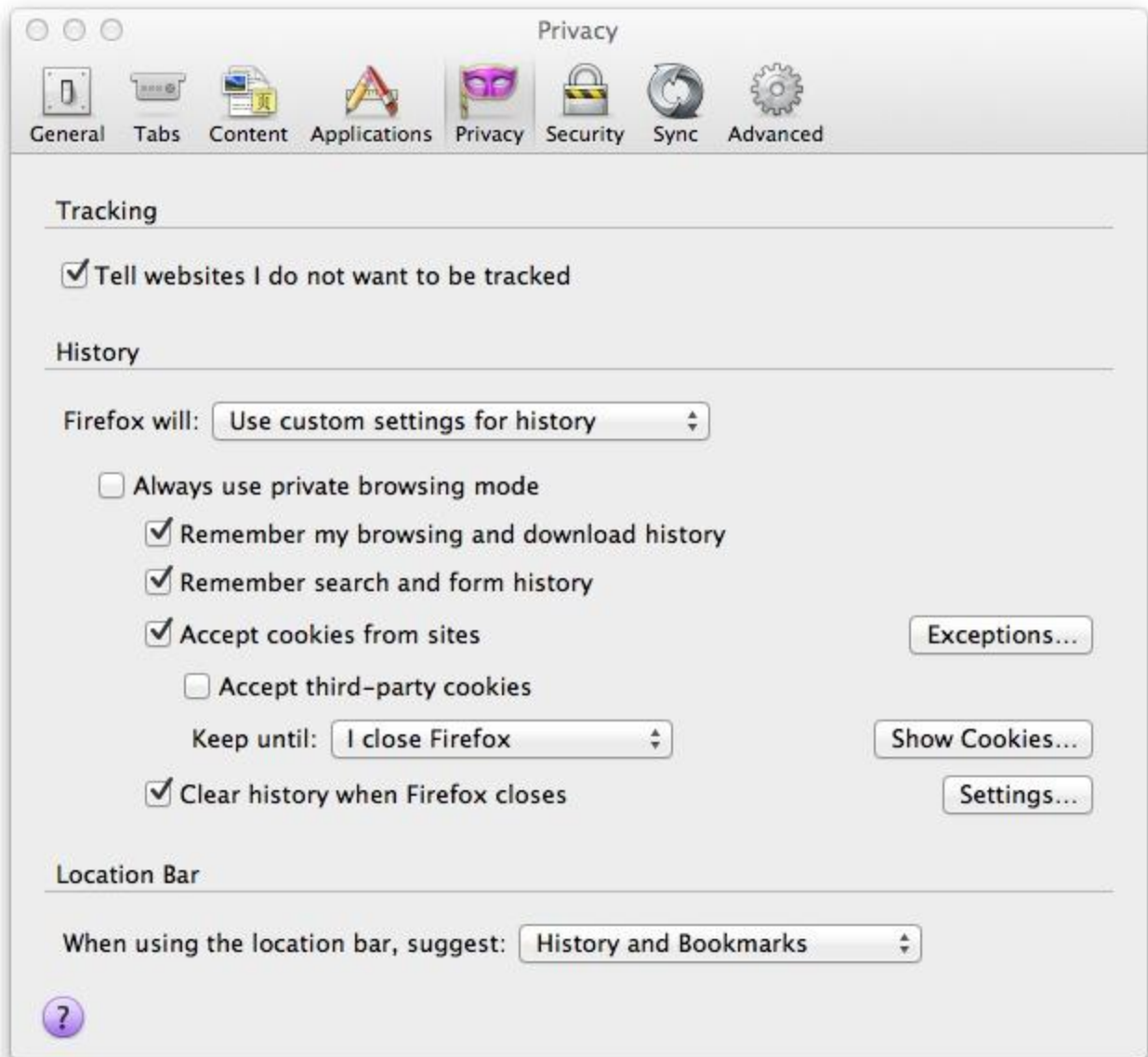
y luego conectarse a cada servicio:



Por eso es muy importante verificar que siempre se esté conectando por una conexión segura (HTTPS) durante toda la sesión. Y usar la opción de Desconectarse (logout) al finalizar.

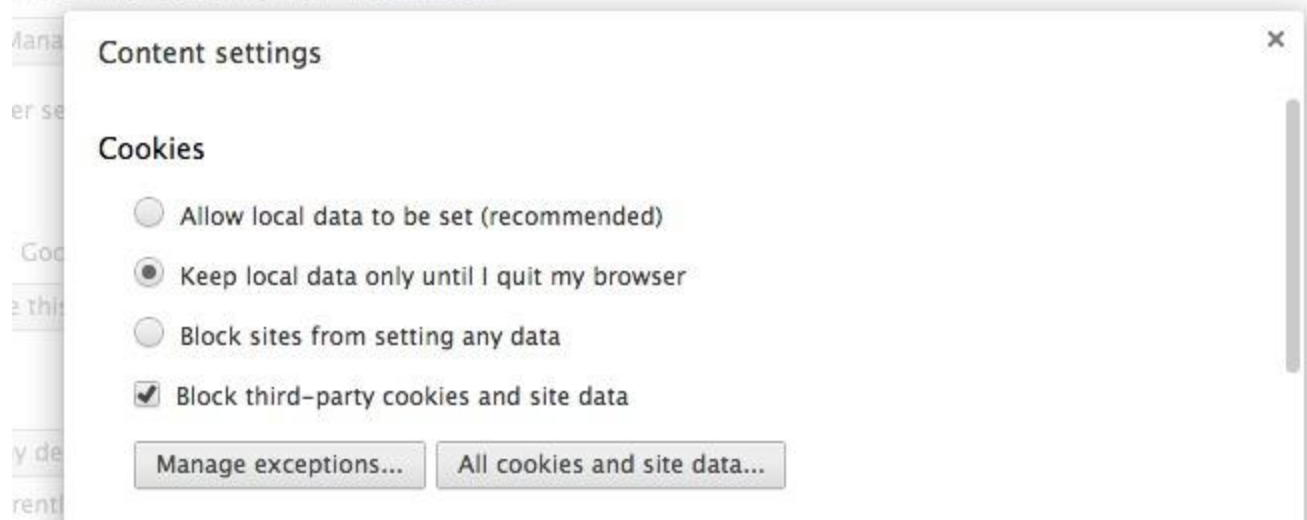
Otra medida de seguridad importante es configurar el browser para que borre el historial y todas las cookies cuando se cierra. Todos los browsers tienen esta funcionalidad y es muy importante activarla.

Firefox:



Google Chrome :

is used when searching from the [omnibox](#).



Content settings ✕

Cookies

- Allow local data to be set (recommended)
- Keep local data only until I quit my browser
- Block sites from setting any data
- Block third-party cookies and site data

[Manage exceptions...](#) [All cookies and site data...](#)