Norton by Symantec

LA BUENA, LA MALA Y LA FASTIDIOSA: ¿SABE LO QUE HACEN SUS APLICACIONES?

Es verdad que hay aplicaciones que son divertidas, productivas y gratuitas, pero también hay otras que pueden causar daños con costes ocultos y presentar comportamientos molestos. Así que ya es hora de dejar de reaccionar frente a los riesgos y empezar a adoptar un nuevo enfoque proactivo con respecto a su protección móvil.

You Tube

Contenido

Actualmente, los dispositivos móviles inteligentes están presentes en cada momento de nuestra vida cotidiana. Hoy en día, casi 1.800 millones de personas, es decir, una cuarta parte de la población mundial, tiene un smartphone.[1] Por ello no es de extrañar que a medida que el uso de los dispositivos móviles aumenta, también lo hace el uso de las aplicaciones.

Los propietarios de los smartphones en todo el mundo pasan actualmente el 86% de su tiempo utilizando aplicaciones, y solo un 14% de ellos emplea las aplicaciones con base en la web.[2] El número medio de aplicaciones instaladas en todo el mundo es de 26 por teléfono, aunque en los 10 países que encabezan el listado esta cifra es de más de 36 aplicaciones instaladas.[3]

Las aplicaciones dan libertad, ya que permiten hacer las mismas cosas que haría en su ordenador pero con su dispositivo móvil. Todo en un modo nuevo y diferente, a medida que avanzamos hacia el Internet de las cosas. Por ejemplo, existen aplicaciones que permiten controlar la temperatura de su salón, encender las luces justo antes de llegar a casa o controlar la seguridad de su hogar frente a los intrusos.

El hecho es que las aplicaciones resultan ser bastante útiles. Si comparamos su teléfono con un vehículo, las aplicaciones serían equivalentes al volante, el acelerador y los intermitentes, y también a la llave que abre la puerta para acceder a toda la información que se encuentra en su dispositivo móvil, así como a toda la información que tenga almacenada en la nube.

Pero claro, los ciber-criminales también han tomado nota de ello. Si se para a pensarlo, su información personal vale bastante dinero y los hackers lo saben, por lo que utilizan cada vez más prácticas ya testadas (como por ejemplo aplicaciones y ransomware falsos) para llegar a los dispositivos móviles, pero tampoco son los únicos… Los desarrolladores de aplicaciones ansiosos por ganar dinero también están al acecho de su información personal, y además sus objetivos no son necesariamente ilegales. Puede que simplemente estén intentando insertar anuncios dirigidos en su barra de notificaciones, aunque sus métodos también pueden conllevar ciertos riesgos.

Seguramente haya muchas partes que estén interesadas en obtener su información privada, por lo que ahora más que nunca resulta primordial saber qué es lo que hacen sus aplicaciones con el fin de poder tomar las medidas necesarias para mantener la seguridad de sus dispositivos móviles.

A decir verdad, hoy en día la localización y el bloqueo de un teléfono perdido o robado simplemente ya no es suficiente. Si bien estas medidas de protección reactivas siguen siendo unas formas importantes de proteger su privacidad, la opción que impera hoy en día es la de contar con una seguridad proactiva. ¿Qué significa esto? Significa que debemos contar con una protección que no solo actúe contra las aplicaciones maliciosas que roban dinero y datos personales, sino que también le dé el poder necesario para tomar decisiones informadas sobre los riesgos potenciales de las aplicaciones que esté descargando, con el fin de valorar si una aplicación gratuita realmente vale la pena.

La protección móvil de hoy en día requiere de un enfoque fresco y preventivo, de modo que pueda acceder libremente y disfrutar de todos los beneficios de su mundo mejorado gracias a las aplicaciones.

[1] eMarketer: www.emarketer.com/Article/Worldwide-Smartphone-Usage-Grow-25-2014/1010920
[2] Flurry: www.flurry.com/bid/109749/Apps-Solidify-Leadership-Six-Years-into-the-Mobile-Revolution#.VH5uBmctDIU
[3] Nuestro Planeta Móvil: www.think.withgoogle.com/mobileplanet/en/

¿Sabe lo que hacen sus aplicaciones? Norton sí lo sabe

La mayoría de los consumidores tienden a percibir las aplicaciones móviles con la misma ingenuidad con la que percibían el software de las aplicaciones de escritorio hace 10 o 15 años. Los consumidores instalan las aplicaciones móviles sin pensar tan siquiera un poco en los riesgos que éstas podrían acarrear, e instalan muchas más aplicaciones que las que realmente necesitan, ya que la descarga se hace con un simple toque.

A muchas aplicaciones (sobre todo las gratuitas) se les da muy bien hablar de los beneficios que ofrecen, pero no tanto de sus verdaderos costes, como por ejemplo amenazas ocultas u otros riesgos potenciales. Las estrategias de Apple con respecto a su sistema operativo iOS, junto con sus fuertes controles sobre lo que accede a la tienda de aplicaciones iTunes, hace que sea realmente difícil toparse con aplicaciones móviles maliciosas. Sin embargo, la naturaleza abierta del sistema operativo Android se puede manipular con mayor facilidad, lo cual puede conllevar diferentes amenazas y riesgos potenciales.

El Informe sobre las amenazas a la seguridad en Internet de Symantec, reveló que el malware móvil del 2013 se desarrolló casi exclusivamente para los sistemas operativos Android, y sobretodo un 32% de esas aplicaciones tenían como finalidad robar la información personal del usuario.[4]

Igualmente, más del 75% de todas las aplicaciones móviles no superaron diferentes pruebas de seguridad básicas, y mostraron una amplia variedad de conductas peligrosas o maliciosas.[5]

Además, Symantec pudo registrar un aumento de un 69% de presencia de malware entre 2012 y 2013.[6]

[4] Informe sobre las amenazas a la seguridad en Internet de Symantec 2014: www.symantec.com/security_response/publications/threatreport.jsp

[5] Gartner: www.gartner.com/newsroom/id/2846017

[6] Norton Mobile Insight/monitorización y análisis de datos de amenazas y respuestas de Symantec a diciembre del 2014

Las aplicaciones malas son justamente eso, malas aplicaciones

Por todo esto resulta muy fácil ver por qué las aplicaciones móviles son un aspecto llamativo para los hackers. El número de usuarios está creciendo rápidamente y la cantidad de información que pueden alcanzar de un solo golpe con una sola aplicación maliciosa es bastante significativa. Y como seguramente ya sabe, los hackers no dejan de mejorar sus artimañas, siempre lo hacen. De hecho están aprendiendo y compartiendo todo su conocimiento, y sus ataques se están haciendo cada vez más sofisticados. Muy a nuestro pesar, los ciber-criminales están aplicando sus eficaces tácticas con los PCs (como por ejemplo phising, software falso y ransomware) a los dispositivos móviles.

Un ejemplo bastante popular fue un timo con una aplicación falsa en la que los phishers ofrecían una aplicación fantasma que supuestamente daría minutos gratis para hablar por móvil. La oferta estaba disponible solo si los usuarios introducían sus datos de inicio de sesión y reenviaban la oferta a 10 amigos. La finalidad del timo era aumentar de forma exponencial el número de las víctimas, robando sus credenciales para obtener otros datos personales.

Otra aplicación falsa copió con una exactitud increíble la aplicación real del Mizhari Bank, uno de los bancos más grandes de Israel. Los hackers la subieron a la tienda de Google Play y los desprevenidos usuarios del banco la descargaron. Cuando abrieron la aplicación e introdujeron su información de acceso, la aplicación se hizo con sus identificadores de usuario. La aplicación envió a continuación un mensaje de error y proporcionó instrucciones a los clientes para volver a instalar la aplicación real del banco, la cual sí funcionaría posteriormente sin ningún problema. La mayoría de los clientes ni siquiera se llegaron a enterar de que en ese momento les habían robado sus identificadores de usuario.

Otra amenaza reciente ha ocurrido con Android. Simplocker es un troyano de ransomware que se propagó mediante una aplicación falsa. Una vez instalado en su dispositivo, cifra (o bloquea) diferentes archivos, y a continuación muestra una alerta falsa del FBI asegurando que se ha encontrado contenido pornográfico ilegal en su dispositivo. A continuación, la aplicación le pide que pague una "multa" de 300 dólares mediante un servicio de pago denominado MoneyPak para poder desbloquear sus archivos.

Guía rápida para identificar las aplicaciones maliciosas

Más de un 20% de los 15 millones de aplicaciones que Norton ha analizado a fecha de hoy son aplicaciones maliciosas.[7] Estas adoptan una gran variedad de formas:

Aplicaciones de rastreo que recogen mensajes de texto y registros de las llamadas, rastrean las coordenadas de su GPS, graban las llamadas, y roban fotos y videos de diferentes dispositivos. El informe de Norton del 2014 mostró que el volumen de las amenazas de rastreo dirigidas al usuario aumentó en el 2013 de un 15% a un 30%.

Aplicaciones ladronas que recogen datos específicos con respecto al dispositivo del usuario como por ejemplo información del dispositivo, datos de configuración y contenido personal.

Aplicaciones infecciosas que ejecutan funciones tradicionales del malware, como por ejemplo instalar puertas traseras y descargadores que permiten que los hackers accedan a su dispositivo.

Aplicaciones de reconfiguración que aumentan los privilegios o modifican la configuración del sistema operativo, lo cual puede permitir que los atacantes accedan a su dispositivo sin mayor dificultad.

Aplicaciones que roban dinero y utilizan números de código cortos, con tarifas costosas mediante mensajes de texto. Una vez instaladas, los hackers crean malware que envía mensajes de texto a esos números desde los dispositivos infectados. Su modus operandi consiste en cobrar a los usuarios una tarifa excesiva a través de sus operadores móviles y son los hackers son quienes reciben el dinero.

Aplicaciones ladronas de factor doble capaces de interceptar mensajes de texto de su banco, las cuales llevan un código de autenticación de un solo uso que permite que los hackers tengan acceso a su cuenta bancaria.

[7] Norton Mobile Insight/monitorización y análisis de datos de amenazas y respuestas de Symantec a diciembre del 2014

El grayware (programas molestos) también puede acarrear riesgos

La línea que separa el software legítimo y el malware sigue siendo difusa y ambigua. Existe una clase de aplicaciones denominadas *grayware* que ocupan el tortuoso terreno intermedio. En estas tierras movedizas intermedias existen muchos desarrolladores no maliciosos. A estos les resulta fácil convencer a los usuarios de que descarguen aplicaciones potencialmente peligrosas capaces de exponer su información y contenido, a menudo utilizando la llamativa fórmula de aplicación "gratis".

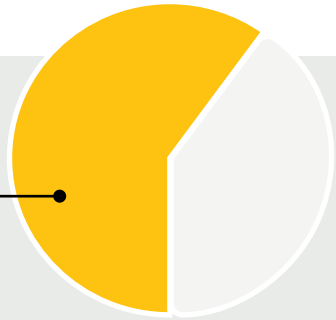
Las aplicaciones de grayware no contienen código malicioso pero sí que pueden comprometer su privacidad y entorpecer el funcionamiento de su dispositivo con anuncios y todo tipo de conductas molestas. Un tipo muy común de *grayware* o también conocido como *publicidad no deseada móvil*, o *madware*, incluye aplicaciones que muestran anuncios en la barra de notificaciones de su teléfono, reemplazan el tono de llamada con anuncios de voz, o lo que es peor aún, exponen datos privados como por ejemplo su número de teléfono o la información de su cuenta de usuario.

Si usted tiene cierto nivel de conocimiento técnico, puede que sea capaz de identificar muchos de estos riesgos, y también si lee cuidadosamente la larga lista de permisos de aplicaciones que está aceptando cuando descargue una aplicación de la tienda de Google Play. Sin embargo no siempre es así, aunque lea todos los permisos, seguirá sin saber cuáles son las conductas reales de tales aplicaciones.

Los estudios de Norton han revelado que más de un

60%

de las aplicaciones Android contienen publicidad no deseada móvil u otro tipo de grayware.[8]



Una vez instalado, el grayware es capaz de rastrear su ubicación o de monitorizar las páginas web que visita y vender tal información a los diferentes comerciantes. En muchos casos, la aplicación cuenta con excusas razonables para recoger datos confidenciales, pero lo más común es que usted no esté al tanto de las acciones de la aplicación, y seguramente haya cierta información personal que no desee compartir con esta. Para verlo más claro, tome como ejemplo a una aplicación que recoge su número de teléfono como identificador único de su dispositivo y lo envía a la red sin ningún tipo de cifrado. Si esto ocurre, su número de teléfono estará disponible para los comerciantes y los artistas del timo prácticamente en cualquier lugar del planeta.

Otro ejemplo puede ser una aplicación que represente riesgos potenciales para su privacidad, al recoger información que no tiene nada que ver con la finalidad de la aplicación en sí. Piense por ejemplo en una aplicación metereológica, ¿para qué necesita acceder a sus contactos o a la información de su agenda electrónica?

Existen otras aplicaciones bastante comunes que por ejemplo agotan su batería, reducen el rendimiento de su dispositivo, o absorben los datos de su red y aumentan los costes de su factura. Técnicamente estas aplicaciones no son consideradas como grayware, pero en cualquier caso son muy fastidiosas, de hecho muchas de ellas se ejecutan a escondidas en un segundo plano. ¿Le parece que la batería de su móvil dura cada vez menos con el paso del tiempo? Puede que la causa sea las aplicaciones que se ha descargado. ¿Le parece que el coste de sus datos es demasiado alto? Adivine la causa: las aplicaciones. Muchas de ellas no hacen más que descargar archivos incluso cuando no están abiertas.

[8] Norton Mobile Insight/monitorización y análisis de datos de amenazas y respuestas de Symantec a diciembre del 2014

Norton y su protección líder, ahora para dispositivos móviles

Usted sabe de la eficacia de Norton en su PC y confía en su potencia. Ahora Norton ha aplicado la misma tecnología de última generación, herramientas de investigación y recursos de inteligencia global para proteger su dispositivo móvil.

La mayoría de los productos de seguridad móvil proporcionan una protección básica, sin embargo Norton va más allá con un servicio basado en una tecnología que le proporciona una protección completa contra las aplicaciones maliciosas y molestas. En Norton hemos aprovechado nuestro conocimiento técnico en materia de seguridad desarrollado durante más de 30 años, así como la base de datos de amenazas más grande del mundo, para ayudarle a estar a salvo contra las amenazas de las aplicaciones Android.

Norton Mobile Insight, siempre alerta

Todos los datos de las aplicaciones Android que recogemos mediante Norton Mobile Insight (por medio de un rastreo constante de más de 200 tiendas de aplicaciones) y la información que reunimos de las aplicaciones a través de la red Norton Community Watch, se introduce en nuestra unidad de procesamiento y se ejecuta mediante una serie sólida de herramientas para identificar aquellas aplicaciones problemáticas.

En primer lugar realizamos un análisis estático, el cual incluye la extracción de datos básicos como por ejemplo el título de la aplicación, la firma del desarrollador, así como la lista de los permisos, la cual normalmente se incluye en el momento de la descarga de la aplicación, y que puede ser excesivamente larga.

A continuación realizamos un análisis más profundo en el código de la aplicación con el fin de visualizar qué interfaz de programación de aplicaciones (Application Programming Interface, API) se va a necesitar. Es decir, ¿la aplicación requiere que la API lea su número de teléfono u otra información privada, y desea también obtener acceso a Internet? Pero no nos detenemos ahí, ya que también nos encargamos de averiguar la localización de la aplicación. ¿Es capaz de instalarse sin colocar un icono en el selector de comandos? Toda esta información proporciona unas claves muy importantes para poder determinar la seguridad de la aplicación.

A continuación, realizamos un importante análisis dinámico, el cual proporciona una visión extraordinaria sobre la privacidad de la aplicación y la fuga de información. Ejecutamos cada aplicación mediante un simulador sincronizado Android, el cual hace que la aplicación piense que está funcionando en el mundo real. Por ejemplo, si una aplicación recoge y envía información del dispositivo o información personal fuera del dispositivo en un segundo plano, probamos si esta podría estar siendo enviada a un tercero no deseado.

Este análisis se realiza de una forma inteligente y automatizada mediante el empleo de flujos de uso real y otras herramientas especializadas. Muchos de nuestros competidores simplemente infieren las conductas de las aplicaciones móviles y reportan sobre los riesgos según los permisos de una aplicación sin llevar a cabo pruebas reales, lo cual puede generar información inexacta o falsas alarmas para el usuario.

Nuestras tecnologías y recursos exclusivos de inteligencia móvil incluyen las siguientes herramientas:

Norton™ Mobile Insight, un sistema dinámico que descarga y analiza de forma constante aplicaciones Android nuevas o actualizadas de más de 200 tiendas de aplicaciones, incluidas Google Play, para generar una inteligencia de aplicaciones continua y única. Esta potente herramienta es capaz de analizar más de 30.000 aplicaciones nuevas al día, y hasta la fecha ha analizado más de 15 millones de aplicaciones.

Norton Community Watch, una red dinámica compuesta por millones de usuarios que nos permite recoger metadatos anónimos y datos de rendimiento a partir de las aplicaciones que se están ejecutando en sus dispositivos Android, incluidos muchos archivos de las aplicaciones nunca antes vistos. La capacidad para aprovechar los datos de la comunidad y para realizar análisis en tiempo real proporciona a Norton Mobile Insight una forma alternativa de entender la conducta de una aplicación una vez instalada, así como los riesgos implícitos de mantenerla en su dispositivo. De hecho, el 25% de las aplicaciones conocidas analizadas por Norton Mobile Insight se obtienen únicamente mediante Norton Community Watch, lo cual significa que tenemos la capacidad de analizar y aprender sobre muchas aplicaciones que no se distribuyen mediante las tiendas de aplicaciones.

La división de Symantec Security Technology and Response (STAR) consiste en un equipo mundial de ingenieros de seguridad, cazadores de virus, analistas de amenazas e investigadores que proporcionan la tecnología de seguridad subyacente, el contenido y la asistencia técnica para todos los productos de seguridad de Symantec, incluidos los diseñados para los dispositivos móviles. Estos expertos son nuestros ojos y oídos, los que investigan el panorama de las amenazas las 24 horas para garantizar su seguridad móvil.

Está claro: a mayor número de datos, mayor es el conocimiento

Por último, la solución de Norton proporciona una ventaja significativa gracias a Symantec Data Analytics Platform (SDAP), uno de los pocos sistemas que cuentan con la potencia y velocidad necesarias para adelantarse al gigantesco crecimiento de las ciber-amenazas, tanto móviles como convencionales.

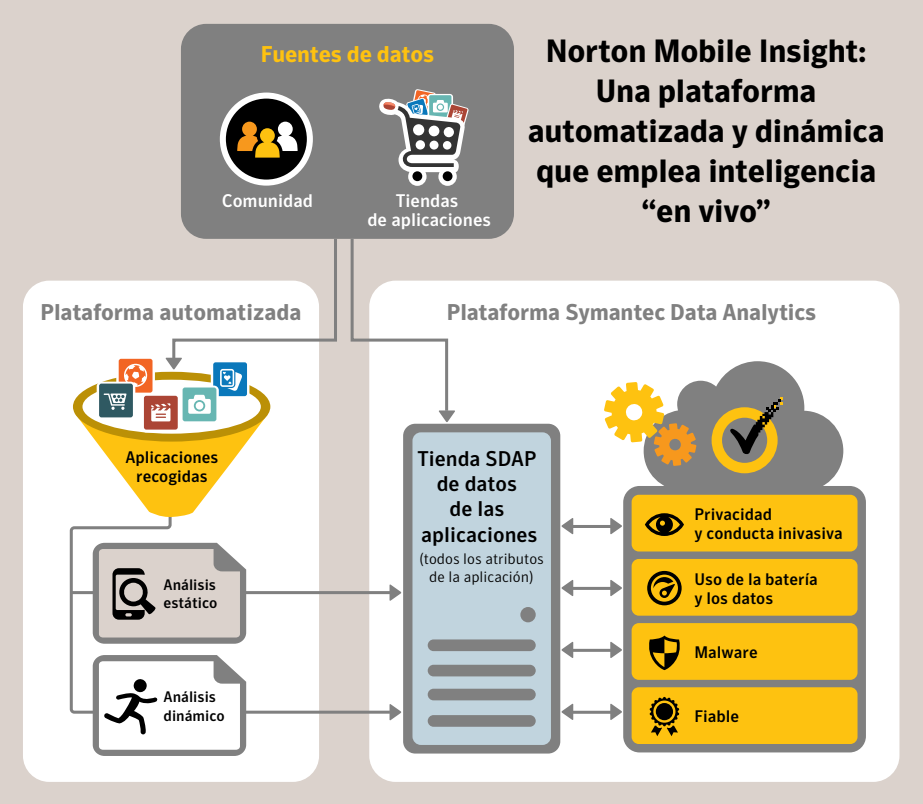
La plataforma SDAP es una base de datos titánica en constante expansión que alberga todos nuestros datos en materia de seguridad. Nuestros datos móviles incluyen alrededor de 1,6 billones de datos, o lo que es lo mismo, 1,6 millones de millones, lo cual es muchísimo. Eso es justo lo que necesitamos para proteger su dispositivo de las amenazas móviles de forma efectiva.

La plataforma SDAP procesa todos los datos de las aplicaciones que recogemos (desde las conductas de las aplicaciones hasta la estabilidad y detalles sobre el rendimiento de estas). Estos datos incluyen información relacionada con la forma en la que la aplicación se ejecuta en el mundo real, cuántas personas de la Norton Community Watch la han utilizado, en qué tiendas de aplicaciones se encuentra y cuántas personas la han descargado.

Una vez contamos y analizamos todos estos datos, determinamos si la aplicación es maliciosa o no. Norton Mobile Insight ha procesado más de 15 millones de aplicaciones hasta la fecha, y continúa procesando más de 30.000 aplicaciones nuevas cada día. Igualmente es capaz de detectar las características y los patrones potencialmente propios de malware, analiza las aplicaciones en búsqueda de conductas sospechosas relacionadas con la privacidad y carácter invasivo, y examina igualmente su uso de la batería y de los datos.

Además está en constante evolución, lo cual le permite adaptarse eficazmente a los cambios del panorama de las amenazas. Es capaz de aprender y evoluciona según los datos que recoge. Por ejemplo, sabe que el tamaño de una aplicación de malware tiende a ser más pequeño que el de las aplicaciones no maliciosas, ya que los desarrolladores de malware normalmente no invierten demasiado tiempo en refinar sus creaciones.

Norton Mobile Insight realiza referencias cruzadas de toda esta información teniendo en cuenta cientos de puntos de datos externos con el fin de averiguar si una aplicación es realmente malware, y establece un nivel de confianza para la seguridad de la aplicación en cuestión. Por otra parte, reconoce os elementos inherentes al malware que un atacante no puede modificar fácilmente, como por ejemplo los patrones del código, las técnicas para llevar a cabo conductas maliciosas, y el estado de la reputación del desarrollador en la comunidad.



Actualmente vivimos en una era en la que las aplicaciones están a la orden del día, por ello es necesario contar con una protección avanzada y proactiva

Norton Mobile Security es un potente producto de suscripción con base en la web diseñado específicamente para protegerlo a usted y a sus dispositivos móviles. Ha sido desarrollado con la avanzada tecnología de Norton Mobile Insight que se ha comentado en este documento. Norton Mobile Security tiene como finalidad ahorrarle tiempo y eliminar las dudas a la hora de identificar las aplicaciones que podrían conllevar diferentes riesgos, tal y como hemos comentado anteriormente.

Uno de los componentes clave de Norton Mobile Security es una herramienta de análisis de aplicaciones denominada App Advisor.

Con la tecnología de Norton Mobile Insight, App Advisor le proporciona una protección proactiva mediante un análisis automático de las aplicaciones en Google Play ANTES de descargarlas (en Android 4.0 o superior, o en Android 4.2 o superior para los dispositivos Samsung). Esta herramienta le notifica si una aplicación contiene código malicioso o si conlleva riesgos para su privacidad, presenta una conducta invasiva, o un uso excesivo de la batería o de los datos. Igualmente analiza automáticamente las aplicaciones de Android que haya descargado anteriormente, o aquellas que haya instalado fuera de una tienda de aplicaciones, con el fin de identificar estos mismos riesgos, y le permite eliminarlas en función de los resultados.

Con un simple paso, sabrá todo lo que necesita para tomar decisiones con respecto a las aplicaciones Android que desea conservar. En resumidas cuentas, podrá decidir si una aplicación realmente “vale la pena”.

Norton Mobile Security también le proporciona otros componentes proactivos de protección para usted y sus dispositivos Android, como Web Protection para protegerle frente a sitios web fraudulentos diseñados para robar su información personal y dinero. También incluye protección remota para la recuperación de su dispositivo Android, iPhone y iPad, para que pueda encontrarlos rápidamente. Incluso podrá guardar sus contactos y restaurarlos en caso de pérdida o robo. Ahora podrá proteger fácilmente todos sus dispositivos con un solo servicio de suscripción con base en la web. Norton Mobile Security le permite aprovechar de forma segura el gran potencial de la comodidad y la libertad móvil sin limitaciones.

A por todas, Norton le protege

La movilidad es parte de su ajetreada vida en red. Sin embargo cada vez dependemos más de estas pequeñas máquinas (sus dispositivos móviles), lo cual hace que sea imperativo reconocer los diferentes riesgos de seguridad móvil a los que se enfrenta, y tomar las medidas necesarias para protegerse.

Ofrecemos además tecnologías de protección Norton Mobile como parte de nuestra plataforma interconectada para nuestras suscripciones a los productos Norton Security y Norton Security con Copia de Seguridad.

Estas suscripciones le proporcionarán a usted, a su familia y a su empresa una protección avanzada especialmente adaptada para sus PCs, Macs, dispositivos Android y iOS con una sola solución fácil de utilizar, completa, y disponible en cualquier momento y en cualquier lugar.

Visítenos en Google Play™ para disfrutar de todas las herramientas de protección avanzadas y proactivas de Norton Mobile Security Premium con una suscripción gratuita durante 30 días. Lo único que tiene que hacer es crear una cuenta Norton, ya que no hace falta incluir los datos de su tarjeta de crédito. Una vez termine el periodo de prueba, podrá adquirir la versión mejorada Premium o seguir usando las funciones GRATUITAS.