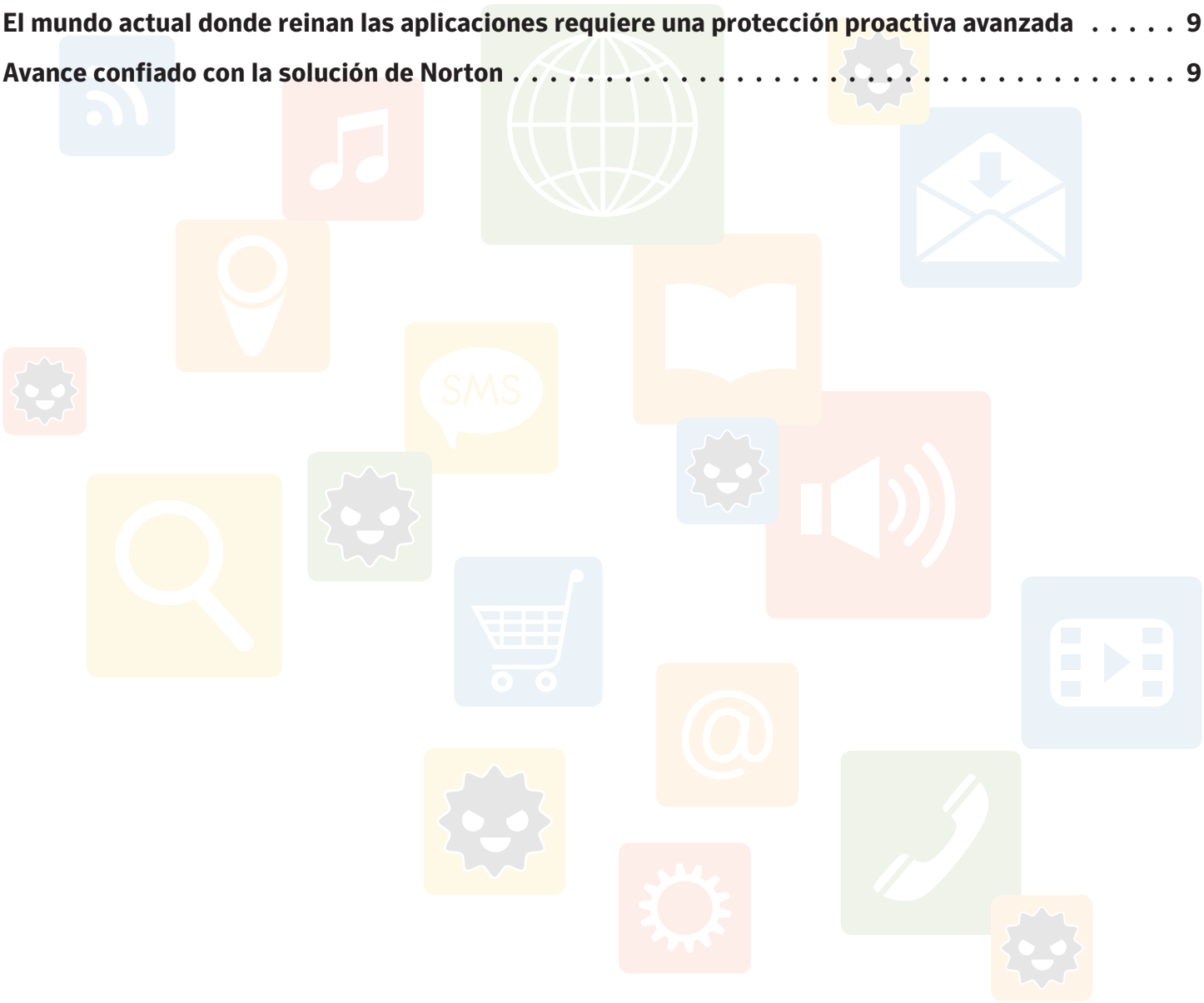
Norton by Symantec

BUENAS, MALAS Y ENGAÑOSAS: ¿SABE REALMENTE QUÉ ESTÁN HACIENDO SUS APLICACIONES?

Las aplicaciones son divertidas, productivas y gratuitas, pero también pueden tener costos ocultos y comportamientos dañinos. Deje de reaccionar a los riesgos y adopte un nuevo enfoque proactivo respecto a su protección móvil.

Contenido



En la actualidad, los dispositivos móviles inteligentes son omnipresentes. En todo el mundo, casi 1.800 millones de personas, o un cuarto de la población mundial, posee un smartphone.[1] Junto con el crecimiento del uso de los dispositivos móviles, crece el uso de las aplicaciones.

Los propietarios de smartphones de todo el mundo ahora emplean un 86 % de su tiempo utilizando aplicaciones y solo un 14 % en la Web.[2] En todo el mundo, el número promedio de aplicaciones instaladas es 26 por teléfono y, en los 10 países principales, es mayor a 35.[3]

Las aplicaciones brindan libertad, ya que le permiten realizar las mismas cosas en su dispositivo móvil que en su PC, y de maneras nuevas y diferentes, a medida que migramos hacia la Internet de las cosas. Por ejemplo, ya puede utilizar aplicaciones para controlar la temperatura de su sala de estar, encender las llaves antes de llegar a su hogar y mantener su casa protegida contra intrusos.

Las aplicaciones permiten que las cosas sucedan. Si su teléfono es el vehículo, las aplicaciones son el volante, el acelerador y la luz de giro. También son la clave que abre la puerta a toda la información que se encuentra en su dispositivo móvil, así como a toda la información que puede tener almacenada en la nube.

Los cibercriminales han tomado nota. Su información personal es valiosa, y los hackers utilizan cada vez más tácticas probadas y eficaces (como aplicaciones falsas y ransomware) para atacar dispositivos móviles. Y no son los únicos. También hay desarrolladores de aplicaciones ávidos de dinero detrás de su información personal. Sus objetivos no son necesariamente ilegales. Tal vez solo intenten insertar publicidad dirigida en su barra de notificaciones. Pero sus métodos pueden ser peligrosos.

Dada la gran cantidad de partes interesadas en obtener su información privada, es más importante que nunca que sepa qué están haciendo sus aplicaciones, y que tome medidas para garantizar la protección de sus dispositivos móviles.

Localizar y bloquear un teléfono perdido o robado no es suficiente. Sí, estas medidas de protección reactivas son importantes. Pero ahora es fundamental optar por una seguridad proactiva. Esto significa una protección no solo contra aplicaciones maliciosas que roban dinero y datos personales, sino también una protección que le permita tomar decisiones informadas sobre el riesgo potencial de las aplicaciones que descarga, y si vale la pena instalar una aplicación gratuita en función del costo final.

La protección móvil ahora exige un nuevo enfoque preventivo para que pueda disfrutar todos los beneficios de nuestro mundo centrado en las aplicaciones sin preocuparse.

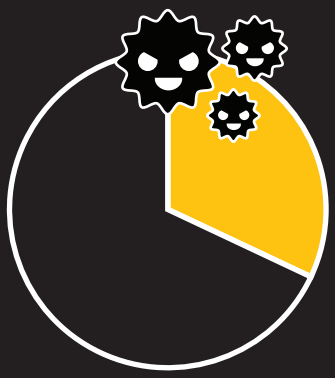
[1] eMarketer: http://www.emarketer.com/Article/Worldwide-Smartphone-Usage-Grow-25-2014/1010920
[2] Flurry: http://www.flurry.com/bid/109749/Apps-Solidify-Leadership-Six-Years-into-the-Mobile-Revolution#.VH5uBmctDIU
[3] Our Mobile Planet: http://think.withgoogle.com/mobileplanet/en/

¿Sabe qué están haciendo sus aplicaciones? Norton sí

La mayoría de los consumidores suelen ver las aplicaciones móviles con el mismo grado de ingenuidad con el que veían al software de aplicaciones de equipos de escritorio hace 10 o 15 años. Instalan aplicaciones móviles sin pensar demasiado, o en absoluto, en los riesgos que pueden representar; e instalan una gran cantidad de ellas porque basta con pulsar una opción para descargarlas.

Las aplicaciones (en especial las gratuitas) describen muy bien los beneficios que brindan, pero no le informan los costos reales. Estos costos pueden tener la forma de amenazas ocultas y otros riesgos potenciales. El espacio aislado del sistema operativo iOS de Apple junto con sus fuertes controles sobre que ingresa en la tienda de aplicaciones iTunes hace que sea difícil encontrar aplicaciones maliciosas. Pero debido a su naturaleza abierta, resulta mucho más simple manipular el sistema operativo Android para ocasionar amenazas y riesgos potenciales.

Según el Informe sobre las Amenazas a la Seguridad en Internet de Symantec, en 2013 el software malicioso móvil se desarrolló casi exclusivamente para el SO Android, donde un 32 % de esas aplicaciones robaba información personal del usuario.[4]



Asimismo, más del 75 % de todas las aplicaciones móviles no superan pruebas de seguridad básicas, ya que ejecutan una variedad de comportamientos maliciosos o peligrosos.[5]

Y Symantec registró un aumento del 69 % en las instancias de software malicioso móvil entre 2012 y 2013.

[4] Informe sobre las Amenazas a la Seguridad en Internet de Symantec de 2014 http://www.symantec.com/security_response/publications/threatreport.jsp
[5] Gartner: http://www.gartner.com/newsroom/id/2846017

Norton by Symantec

Las aplicaciones dañinas no son más que eso

Es fácil saber por qué las aplicaciones móviles son atractivas para los hackers. La base de usuarios está creciendo rápidamente y la cantidad de información que se puede obtener una vez instalada una aplicación maliciosa es considerable. Y, como sucede siempre, los hackers son cada vez mejores. Están aprendiendo y compartiendo información y sus ataques son cada vez más sofisticados. Los cibercriminales están aplicando las tácticas probadas que ya empleaban en PC (como phishing, software falso y ransomware) a los dispositivos móviles.

En una estafa con una aplicación falsa, los phishers ofrecieron una aplicación falsa que alegaba dar minutos gratuitos de llamadas. La oferta estaba disponible solo si los usuarios ingresaban sus credenciales de inicio de sesión y reenviaban la oferta a 10 amigos. La estafa tenía como objetivo aumentar exponencialmente el número de víctimas, robar credenciales y captar otros datos personales.

Otra aplicación falsa era una copia fiel de la aplicación real de Mizrahi Bank, uno de los bancos más grandes de Israel. Los hackers la subieron a la tienda Google Play y clientes bancarios la descargaron sin sospechar. Cuando abrieron la aplicación e ingresaron su información de inicio de sesión, la aplicación captaba sus Id. de usuario. La aplicación luego enviaba un mensaje de error y solicitaba a los clientes que volvieran a instalar la aplicación real del banco, que luego funcionaba correctamente. La mayoría de los clientes no sospechaban que sus Id. de usuario habían sido robados.

Otra amenaza reciente es Android. Simplocker, un ransomware troyano que se entregaba mediante una aplicación falsa. Una vez instalada en su dispositivo, cifra (o bloquea) los archivos y luego muestra una alerta falsa del FBI que informa que se encontró contenido pornográfico ilegal en su dispositivo. Después se le solicita que pague una “multa” de 300 USD mediante un servicio de pago denominado MoneyPak para desbloquear sus archivos.

Guía rápida sobre aplicaciones maliciosas

Más del 20 % de las 15 millones de aplicaciones analizadas hasta la fecha por Norton son aplicaciones maliciosas. Existen varios tipos:

Aplicaciones de seguimiento: recopilan registros de llamadas y mensajes de texto, realizan seguimientos de coordinadas GPS, graban llamadas y roban fotos y videos de los dispositivos. Según el Informe de Norton de 2014, el volumen de amenazas que realizan un seguimiento del usuario aumentó en 2013 de un 15 % a un 30 %.

Aplicaciones de robo: recopilan datos específicos del dispositivo o del usuario, como información del dispositivo, datos de configuración o contenido personal.

Aplicaciones de infección: ejecutan funciones de software malicioso tradicionales, como instalar puertas traseras y descargadores que les dan a los hackers acceso a su dispositivo.

Aplicaciones de reconfiguración: aumentan los privilegios o modifican la configuración en el sistema operativo, lo que puede facilitarles el acceso a los atacantes.

Aplicaciones de robo de dinero: utilizan números de mensajes de texto de tarifa premium y código corto. Luego, los hackers crean software malicioso que envía mensajes de texto a esos números desde dispositivos infectados. Los usuarios reciben la factura de los operadores y el hacker se queda con el dinero.

Aplicaciones de robo de dos factores: pueden interceptar un mensaje de texto de su banco con un código de autenticación de un solo uso, que podría darles a los hackers acceso a su cuenta bancaria.

El grayware también puede ser peligroso

La línea entre el software legítimo y el software malicioso no está trazada claramente. Existe una clase de aplicaciones denominada *grayware* que ocupa una zona gris. En esta zona gris, se encuentran muchos desarrolladores no maliciosos que pueden persuadir fácilmente a los usuarios de descargar aplicaciones potencialmente peligrosas que exponen información y contenido, por lo general, mediante el atractivo de una aplicación gratuita.

Las aplicaciones de tipo Grayware no contienen código malicioso, pero pueden comprometer su privacidad y afectar el funcionamiento del dispositivo con publicidad y todo tipo de comportamiento molesto. Un tipo común de grayware denominado *publicidad no deseada móvil* o *madware*, incluye aplicaciones que muestran publicidades en la barra de notificaciones de un teléfono, reemplazan el tono de marcado con publicidades de voz o, en el peor de los casos, exponen números de teléfono o información de cuentas de usuarios.

Muchos de estos riesgos se pueden detectar si se cuenta con cierto grado de conocimiento técnico y se lee atentamente la larga lista de permisos de aplicaciones que se aceptan cuando se descarga una aplicación de la tienda Google Play. Pero ese no siempre es el caso. Incluso si efectivamente lee los permisos, eso no le permite conocer todos los comportamientos de la aplicación.

Un estudio de investigación de Norton indica que más del

60 %

de las aplicaciones para Android contienen publicidad no deseada u otro grayware.

Una vez instalada, el grayware podría rastrear su ubicación o supervisar su navegación web y vender la información a profesionales de marketing. En muchos casos, una aplicación tiene una excusa razonable para recopilar algunos datos confidenciales, pero por lo general usted no conoce su comportamiento y es muy probable que no se sienta cómodo compartiendo cierta información personal con esa aplicación específica. Tomemos, por ejemplo, una aplicación que recopila su número de teléfono como Id. único de su dispositivo y lo envía a través de la red sin cifrarlo. Repentinamente, su número de teléfono está a disposición de profesionales de marketing y estafadores malintencionados prácticamente en todas partes.

O una aplicación puede presentar un riesgo potencial para la privacidad mediante la recopilación de información que no parece razonable dado el objetivo de la aplicación. Por ejemplo, ¿por qué una aplicación meteorológica necesita acceso a sus contactos o a la información de su calendario?

Igual de comunes son las aplicaciones que agotan la batería, afectan el rendimiento del dispositivo o descargan datos de la red y encarecen su factura telefónica. Si bien estas aplicaciones no son técnicamente grayware, sin dudas son muy molestas. Muchas de ellas se ejecutan a escondidas en segundo plano. ¿Nota que la vida de la batería de su dispositivo disminuye con el tiempo? Las aplicaciones podrían ser el motivo. ¿Paga un monto inesperadamente elevado por descarga de datos? Una vez más, puede deberse a las aplicaciones. Muchas descargan una gran cantidad de datos incluso cuando no están abiertas.

Norton ofrece protección líder para dispositivos móviles

Usted confía en Norton para proteger su PC. Aplicamos la misma tecnología de vanguardia, las capacidades exhaustivas de investigación y los recursos de inteligencia global para proteger su dispositivo móvil.

La mayoría de los productos de seguridad móvil proporcionan protección básica.

Hacemos todo lo necesario para brindar tecnología que lo proteja completamente contra aplicaciones maliciosas y molestas. Aprovechamos nuestros 30 años de experiencia en materia de seguridad y la base de datos de amenazas más grande del mundo para mantenerlo protegido contra amenazas de aplicaciones para Android.

Norton Mobile Insight nunca duerme

Todos los datos de aplicaciones para Android que recopilamos mediante Norton Mobile Insight (gracias al rastreo constante de 200 tiendas de aplicaciones y la compilación de información de aplicaciones de la red Norton Community Watch) se ingresan en nuestro canal de procesamiento y se ejecutan mediante un sólido conjunto de aplicaciones para identificar a las que representan problemas.

Primero, realizamos un análisis estático, que incluye la extracción de datos básicos como el nombre de la aplicación, la firma del desarrollador y la lista de permisos, que suelen estar presente en el momento en que se descarga una aplicación y puede ser excesivamente larga.

Luego, realizamos un análisis más exhaustivo del código de la aplicación para ver a qué interfaces para programación de aplicaciones (API) internas se llamará. Por ejemplo, se debe determinar si la aplicación llama a una o más API para leer su número de teléfono y otra información privada y, luego, acceder a Internet. Y la interrogación no termina allí. Averiguamos si la aplicación está localizada. ¿Se instala sin crear un icono en el iniciador? Esta información proporciona pistas importantes respecto de la seguridad de la aplicación.

Después, ejecutamos un importante análisis dinámico, que nos ofrece una visión sin precedentes sobre la fuga de información y la privacidad de la aplicación. Ejecutamos todas las aplicaciones en un emulador Android instrumentado, lo que hace que la aplicación crea que se está ejecutando en el mundo real. Por ejemplo, si una aplicación recopila y envía información personal o del dispositivo en segundo plano, podría estar yendo a un tercero no deseado.

Realizamos este análisis de una manera inteligente y automatizada con funciones y flujos de uso reales. Muchos de nuestros competidores solo infieren comportamientos de las aplicaciones móviles e informan riesgos en función de los permisos de las aplicaciones sin realizar pruebas, lo que puede ocasionar que el usuario reciba información poco precisa o falsas alarmas.

Nuestros recursos y tecnologías de inteligencia móvil exclusivos incluyen lo siguiente:

Norton™ Mobile Insight es un sistema dinámico que descarga y analiza constantemente aplicaciones para Android nuevas o actualizadas de más de 200 tiendas de aplicaciones, incluida Google Play, para generar una inteligencia sobre aplicaciones única y constante. Analizamos más de 30 000 aplicaciones nuevas cada día y hemos analizado más de 15 millones de aplicaciones hasta la fecha.

Norton Community Watch es una red vibrante que consta de millones de usuarios que nos permiten recopilar metadatos anónimos y datos de rendimiento de aplicaciones en ejecución en sus dispositivos Android, lo que incluye muchos archivos de aplicaciones desconocidos. Aprovechar los datos de esta comunidad y ejecutar análisis en tiempo real brinda a Norton Mobile Insight otra manera de comprender el comportamiento de una aplicación una vez que está instalada, así como los riesgos que implica tenerla en el dispositivo. De hecho, un 25 % de las aplicaciones conocidas analizadas por Norton Mobile Insight se recopilan solo de Norton Community Watch, lo que significa que estamos analizando y obteniendo información sobre muchas aplicaciones que no se distribuyen mediante tiendas de aplicaciones.

La división Security Technology and Response (STAR) de Symantec consta de un equipo global de ingenieros de seguridad, cazadores de virus, analistas de amenazas e investigadores que proporciona tecnología de seguridad, contenido y soporte subyacentes para todos los productos de seguridad de Symantec, incluidos productos para dispositivos móviles. Estos expertos son nuestros ojos y oídos e inspeccionan el panorama de amenazas día y noche para mantenerlo seguro.

Datos: Cuanto más tiene, más sabe

Por último, la solución Norton cuenta con la gran ventaja que brinda la plataforma de análisis de datos de Symantec (SDAP), uno de los pocos sistemas que tienen la habilidad y la eficacia necesarias para mantenerse a la par del enorme crecimiento de las amenazas cibernéticas, de dispositivos móviles y de otro tipo.

La plataforma SDAP es una enorme base de datos en continua expansión que aloja todos nuestros datos de seguridad. Nuestros datos móviles incluyen cerca de 1,6 billones de datos individuales. Son muchísimos datos. Pero eso es lo que se necesita para proteger su dispositivo de amenazas móviles.

Todos los datos de aplicaciones que recopilamos (desde comportamientos de aplicaciones, hasta estabilidad de aplicaciones y detalles de rendimiento) son procesados por la plataforma SDAP. Estos datos incluyen información sobre cómo se comporta la aplicación en el mundo real, cuántas personas de Norton Community Watch la han utilizado, en qué tiendas de aplicaciones se encuentra y cuántas personas la han descargado.

Analizamos todos los datos y luego determinamos si la aplicación es maliciosa. Norton Mobile Insight ha procesado más de 15 millones de aplicaciones hasta la fecha y procesa 30 000 aplicaciones nuevas cada día. Detecta las funciones y los patrones que indican la presencia de software malicioso, comprueba si las aplicaciones contienen comportamiento intrusivo o comportamiento de privacidad sospechoso y examina el uso de los datos y la batería.

Y su inteligencia evoluciona constantemente, a medida que cambia el panorama de amenazas. Aprende y evoluciona en función de los nuevos datos que recopila. Por ejemplo, sabe que el tamaño de las aplicaciones con software malicioso tiende a ser menor que el de las aplicaciones seguras porque los desarrolladores de software malicioso no suelen dedicar demasiado tiempo a perfeccionar sus creaciones.

Luego, Norton Mobile Insight compara toda esta información con otros cientos puntos de datos para comprobar si la aplicación contiene software malicioso y establece un nivel de confianza para la seguridad de la aplicación. Reconoce elementos inherentes al software malicioso que un atacante no puede modificar fácilmente, como patrones de código, técnicas para ejecutar comportamientos maliciosos y el estado de la reputación del desarrollador en la comunidad.

El mundo actual donde reinan las aplicaciones requiere una protección proactiva avanzada

Norton Mobile Security es una eficaz suscripción basada en Web diseñada para protegerlo a usted y a sus dispositivos móviles. Cuenta con la tecnología avanzada Norton Mobile Insight que se analiza en este documento. Norton Mobile Security está diseñada para que ahorre tiempo y elimine las conjeturas cuando identifique aplicaciones con todos los riesgos que se analizan en este documento.

La clave de Norton Mobile Security es una función de análisis de aplicaciones llamada App Advisor.

Con tecnología Norton Mobile Insight, App Advisor proporciona protección proactiva ya que permite analizar automáticamente aplicaciones en Google Play antes de descargarlas (en Android 4.0 o posterior, o Android 4.2 o posterior en dispositivos Samsung). Le indicará si las aplicaciones contienen código malicioso, riesgos potenciales para la privacidad o comportamiento intrusivo, o si hacen uso intensivo de la batería o de los datos. Además, analiza automáticamente las aplicaciones para Android o las aplicaciones que no se hayan instalado desde una tienda de aplicaciones descargadas anteriormente en busca de estos mismos riesgos y le permite eliminarlos si lo desea.

En un simple paso, usted puede tomar decisiones informadas respecto de las aplicaciones para Android. Puede decidir si vale la pena instalar una aplicación específica en función del costo.

Norton Mobile Security también proporciona otros componentes de protección proactiva para usted y sus dispositivos Android, como la protección web para protegerlo de sitios web fraudulentos diseñados para robarle dinero e información personal. También incluye protección de recuperación remota de dispositivos Android, iPhone y iPad a fin de que pueda encontrarlos rápidamente. Incluso puede guardar su información de contacto y restaurarla en caso de pérdida o robo. Ahora es fácil proteger todos los dispositivos con un servicio de suscripción basado en Web. Norton Mobile Security le permite aprovechar el gran potencial de la comodidad y la libertad móvil sin limitaciones y de forma segura.

Avance confiado con la solución de Norton

La movilidad es un componente esencial de su vida atareada y conectada. Pero el uso cada vez mayor de estos pequeños equipos, los dispositivos móviles, hace que sea indispensable reconocer los riesgos para la seguridad móvil y tomar medidas de protección.

También ofrecemos tecnologías de protección de Norton Mobile como parte de nuestras suscripciones de productos Norton Security, Norton Security con Backup y Norton Small Business de plataformas cruzadas. Estas tres suscripciones le brindan a usted, su familia y su empresa protección adaptada a sus PCs, Macs y dispositivos Android e iOS con una solución integral y fácil de usar en cualquier momento y lugar.

Visítenos en Google Play™ para disfrutar de todas las funciones avanzadas de protección proactiva de la suscripción de Norton Mobile Security Premium gratis durante 30 días. Solo debe crear una cuenta de Norton, sin necesidad de ingresar los datos de una tarjeta de crédito. Una vez que finalice el período de prueba, puede actualizarse a la versión Premium o seguir usando las funciones gratuitas.