Norton by Symantec

GUT, SCHLECHT ODER TRICKREICH: WISSEN SIE WIRKLICH, WAS IHRE APPS ALLES MACHEN?

Apps bringen Spaß, machen produktiver und sind oft gratis. Aber Sie können auch viel Ärger bereiten – durch versteckte Kosten und unerwünschtes Verhalten. Statt nur auf Risiken zu reagieren, sollten Sie beim Schutz Ihrer mobilen Welt auf ein neues, proaktives Konzept setzen.

Inhalt

Intelligente Mobilgeräte sind heute allgegenwärtig. Weltweit besitzen fast 1,8 Milliarden Menschen ein Smartphone – das ist ein Viertel der Weltbevölkerung.[1] Und mit den Mobilgeräten breitet sich auch die Nutzung von Apps aus.

Smartphone-Besitzer auf der ganzen Welt verbringen heute 86 Prozent ihrer Zeit mit Apps und nur 14 Prozent im Web.[2] Weltweit sind auf jedem Gerät im Durchschnitt 26 Apps installiert – und in den zehn führenden Ländern sogar mehr als 35.[3]

Apps stehen für die Freiheit, auf Mobilgeräten das gleiche zu tun wie am PC. Und sie sind Wegbereiter für das Internet der Dinge, das ganz neue und andere Möglichkeiten bietet. Bereits heute können Sie Apps nutzen, um die Temperatur im Wohnzimmer zu regeln, das Licht einzuschalten, bevor Sie heimkommen, und Ihr Zuhause vor Eindringlingen zu schützen.

Apps bringen Sie ans Ziel. Ohne sie wäre Ihr Smartphone so nutzlos wie ein Auto ohne Lenkrad, Gaspedal und Blinker. Und damit nicht genug – sie sind auch der Schlüssel zu allen Informationen, die Sie auf Ihrem mobilen Gerät oder in der Cloud gespeichert haben.

Internetkriminelle wissen das ganz genau. Ihre persönlichen Daten sind bares Geld wert. Hacker setzen bewährte Taktiken (wie gefälschte Apps und Ransomware) immer öfter ein, um Mobilgeräte ins Visier zu nehmen. Und sie sind nicht die Einzigen. Auch profithungrige App-Entwickler interessieren sich brennend für Ihre persönlichen Daten. Dabei verfolgen sie gar nicht unbedingt illegale Ziele. Sie versuchen vielleicht einfach nur, personalisierte Anzeigen in die Benachrichtigungsleiste Ihres Smartphones einzublenden. Aber ihre Methoden können Risiken darstellen.

Es gibt also jede Menge Leute, die sich Zugang zu Ihren privaten Daten verschaffen möchten. Deshalb ist es wichtiger denn je, dass Sie wissen, was Ihre Apps tun, und Maßnahmen zur Sicherung Ihrer Mobilgeräte ergreifen.

Es genügt heute nicht mehr, ein gestohlenes Smartphone zu orten und zu sperren. Diese reaktiven Schutzmaßnahmen sind zweifellos wichtig, aber das Gebot der Stunde ist proaktive Sicherheit. Bei diesem Ansatz werden Sie nicht nur vor bösartigen Apps geschützt, die Geld und persönliche Daten stehlen. Sie erhalten auch Aufschluss über die potenziellen Risiken der von Ihnen heruntergeladenen Apps. So können Sie beurteilen, welchen Preis Sie für eine Gratis-App schlimmstenfalls zahlen müssten, und entscheiden, ob sie Ihnen das wirklich wert ist.

Schutz für Mobilgeräte erfordert heute ein innovatives Konzept, das auf Prävention setzt – damit Sie alle Vorteile, die Ihnen die Welt der Apps verspricht, beruhigt genießen können.

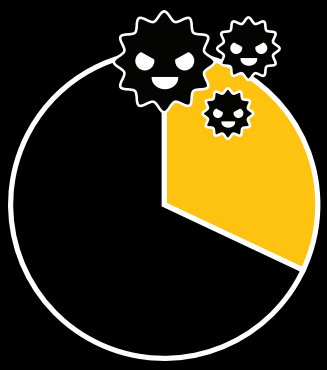
[1] eMarketer: www.emarketer.com/Article/Worldwide-Smartphone-Usage-Grow-25-2014/1010920
[2] Flurry: www.flurry.com/bid/109749/Apps-Solidify-Leadership-Six-Years-into-the-Mobile-Revolution#.VH5uBmctDIU
[3] Our Mobile Planet: www.think.withgoogle.com/mobileplanet/en/

Wissen Sie wirklich, was Ihre Apps alles machen?

Die meisten Nutzer sind bei mobilen Apps genau so unvorsichtig wie vor 10 oder 15 Jahren bei PC-Programmen. Sie installieren mobile Apps, ohne groß an die damit verbundenen Risiken zu denken – und das in großer Zahl, weil ein Fingertipp zum Herunterladen genügt.

Apps – vor allem die kostenlosen – verraten Ihnen sehr viel über ihre Vorzüge, aber nichts über den Preis, den Sie womöglich dafür zahlen: versteckte Bedrohungen und andere potenzielle Risiken. Apple setzt auf eine isolierte Umgebung (Sandboxing) für das Betriebssystem iOS und kontrolliert zudem streng, was über den iTunes App Store angeboten werden darf. Das senkt die Gefahr, an ein Schadprogramm zu geraten. Das Betriebssystem Android ist hingegen aufgrund seiner Offenheit anfälliger für Manipulationen, die Bedrohungen und potenzielle Risiken verursachen.

Laut dem Symantec Internet Security Threat Report wurde Malware für Mobilgeräte im Jahr 2013 fast ausschließlich für Android entwickelt, wobei 32 Prozent dieser schädlichen Apps die persönlichen Daten der Benutzer stehlen.[4]



Mehr als 75 Prozent aller mobilen Apps fallen aufgrund riskanten oder bösartigen Verhaltens bei elementaren Sicherheitstests durch.[5]

Und Symantec verzeichnet bei mobiler Malware von 2012 auf 2013 einen Anstieg um 69 Prozent.[6]

[4] 2014 Symantec Internet Security Threat Report: www.symantec.com/security_response/publications/threatreport.jsp

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

[6] Beobachtungs- und Analysedaten von Norton Mobile Insight/Symantec Threat and Response, Stand Dezember 2014.

Erwarten Sie nichts Gutes von bösartigen Apps

Mobile Apps sind für Hacker sehr attraktiv – und es ist nicht schwer zu verstehen, warum. Die Nutzerbasis wächst schnell. Eine bösartige App kann zahlreiche Informationen abgreifen, wenn sie erst einmal installiert ist. Und die Hacker werden immer besser. Sie lernen und tauschen sich aus, und ihre Angriffe werden immer raffinierter. Internetkriminelle übertragen ihre bewährten Taktiken (wie Phishing, gefälschte Software und Ransomware) vom PC auf Mobilgeräte.

In einem Fall boten Phishing-Angreifer eine gefälschte Smartphone-App an, die kostenlose Gesprächsminuten versprach. Allerdings galt das Angebot nur, wenn ein Benutzer Login-Daten eingab und das Angebot an zehn Freunde weiterleitete. Der Betrug zielte darauf, die Anzahl der Opfer zu vervielfachen, Anmeldedaten zu stehlen und andere persönliche Informationen zu sammeln.

Eine weitere gefälschte App kopierte detailgenau die echte App der Mizrahi Bank, einer der größten Banken in Israel. Hacker luden sie in den Google Play Store hoch, wo sie von nichtsahnenden Bankkunden heruntergeladen wurde. Sobald sie die App öffneten und ihre Anmeldedaten eingaben, wurden diese abgegriffen. Dann gab die App eine Fehlermeldung aus, die die Benutzer anwies, die echte App der Bank erneut zu installieren, die anschließend reibungslos funktionierte. Die meisten Kunden bekamen es nie mit, dass ihre Benutzerkennungen gestohlen worden waren.

Eine weitere aktuelle Bedrohung ist Android.Simplocker, ein Ransomware-Trojaner, der über eine gefälschte App eingeschleust wird. Einmal installiert, verschlüsselt (oder sperrt) er Dateien und zeigt eine gefälschte FBI-Warnmeldung an, die behauptet, dass auf dem Gerät illegale pornografische Inhalte gefunden wurden. Der Benutzer wird angewiesen, über den Zahlungsdienstleister MoneyPak 300 US-Dollar „Strafe“ zu zahlen, damit die Dateien wieder freigegeben werden.

Bösartige Apps im Überblick

Über 20 Prozent der 15 Millionen von Norton bisher analysierten Apps sind Schadprogramme.[7] Sie kommen in vielen unterschiedlichen Formen vor:

Spionierende Apps lesen SMS und Anrufprotokolle aus, verfolgen die GPS-Koordinaten, zeichnen Telefongespräche auf und stehlen Fotos und Videos von den Geräten. Nach Erkenntnissen des Norton-Berichts 2014 sind die Bedrohungen durch das Ausspionieren von Benutzern im Jahr 2013 von 15 auf 30 Prozent gestiegen.

Stehlende Apps entwenden geräte- und benutzerspezifische Angaben wie Informationen zum Gerät, Konfigurationsdaten und persönliche Inhalte.

Infizierende Apps führen klassische Malware-Funktionen aus. Sie installieren z. B. Backdoors und Downloader, über die Hacker Zugang zu Ihrem Gerät erhalten.

Rekonfigurierende Apps manipulieren die Zugriffsrechte oder Einstellungen des Betriebssystems. Dies kann Angreifern Tür und Tor öffnen.

Gelddiebstahl-Apps nutzen gebührenpflichtige Premium-SMS-Nummern. Hacker verbreiten Malware, die von den infizierten Geräten aus SMS-Nachrichten an diese Nummern verschickt. Den Benutzern wird eine saftige Telefonrechnung präsentiert, während der Hacker das Geld einsteckt.

Zwei-Faktor-Diebstahl-Apps sind in der Lage, eine SMS Ihrer Bank mit einer TAN für eine einmalige Transaktion abzufangen. Damit können sich Hacker Zugang zu Ihrem Bankkonto verschaffen.

[7] Beobachtungs- und Analysedaten von Norton Mobile Insight/Symantec Threat and Response, Stand Dezember 2014.

Auch Grayware kann riskant sein

Legitime Software und Malware lassen sich nicht scharf voneinander abgrenzen. Apps, die sich in der Grauzone zwischen beiden befinden, werden als *Grayware* bezeichnet. Viele davon stammen von Entwicklern, die zwar keine kriminellen Absichten verfolgen, aber Benutzer mit „kostenlosen“ Apps locken, die sie gern herunterladen – auch wenn sie damit die Preisgabe von Informationen und Inhalten riskieren.

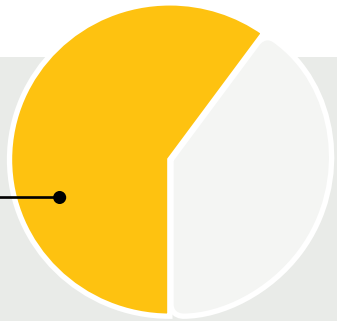
Grayware-Apps enthalten keinen Schadcode. Sie können jedoch gleichwohl Ihre Privatsphäre kompromittieren und Ihr Gerät durch unerwünschte Werbeeinblendungen und andere störende Verhaltensweisen beeinträchtigen. Eine verbreitete Art der *Grayware* ist *Adware für Mobilgeräte*, die auch als *Madware* bezeichnet wird. In diese Kategorie fallen Apps, die Werbeanzeigen in der Benachrichtigungsleiste eines Smartphones einblenden, den Wählton durch Werbespots ersetzen oder gar private Informationen wie Telefonnummern und Kontodaten offenlegen.

Wenn Sie über umfassendes technisches Wissen verfügen und die lange Liste der App-Berechtigungen sorgfältig durchlesen, könnten Sie viele dieser Risiken theoretisch bereits beim Download der App aus dem Google Play Store erkennen. Leider ist das jedoch nicht immer der Fall.

Laut einer Studie von Norton enthalten über

60 Prozent

aller Android-Apps Adware oder Grayware.[8]



Und selbst wenn Sie die Berechtigungen lesen, wissen Sie damit noch nicht, wie sich die App tatsächlich verhält.

Eine einmal installierte Grayware-App kann beispielsweise Ihren Standort oder Ihren Browserverlauf aufzeichnen und diese Informationen zu Marketingzwecken verkaufen. In vielen Fällen gibt es einen nachvollziehbaren Grund dafür, dass eine App manche sensiblen Daten erfasst. Aber meist wissen Sie nichts über das Verhalten der betreffenden App und hätten vermutlich kein gutes Gefühl dabei, ihr bestimmte persönliche Informationen zugänglich zu machen. Ein Beispiel dafür sind etwa Apps, die Ihre Telefonnummer als eindeutige Kennung Ihres Gerätes erfassen und unverschlüsselt über das Netz senden – so dass Vermarkter und Betrüger an praktisch jedem beliebigen Ort darauf zugreifen können.

Oder Apps, die Informationen erfassen, die sich mit ihrem vorgesehenen Zweck nicht plausibel rechtfertigen lassen und damit potenziell Ihre Privatsphäre gefährden. Weshalb sollte beispielsweise eine Wetter-App auf Ihre Kontakte oder Kalenderinformationen zugreifen müssen?

Häufig kommt es auch vor, dass Apps den Akku stark belasten, die Geräteleistung beeinträchtigen oder große Datenmengen über das Netz herunterladen und Ihre Rechnung in die Höhe treiben. Solche Anwendungen sind strenggenommen keine Grayware, aber zweifellos ärgerlich. Oft werden sie unbemerkt im Hintergrund ausgeführt. Stellen Sie fest, dass die Akkulaufzeit Ihres Geräts mit der Zeit immer kürzer wird? Die Ursache dafür sind möglicherweise Apps. Verursacht Ihr Datenverbrauch überraschend hohe Kosten? Auch hierfür können Apps verantwortlich sein. Viele laden selbst dann große Datenmengen herunter, wenn sie nicht ausgeführt werden.

[8] Beobachtungs- und Analysedaten von Norton Mobile Insight/Symantec Threat and Response, Stand Dezember 2014.

Norton bietet bewährten Schutz – auch für Mobilgeräte

Sie vertrauen Norton, wenn es um den Schutz Ihres PCs geht. Die gleiche Spitzentechnologie, umfassende Forschungskapazitäten und globale Informationsinfrastruktur setzen wir ebenfalls ein, um Ihr Mobilgerät zu schützen.

Die meisten der momentan erhältlichen Sicherheitsprodukte für Mobilgeräte bieten Basisschutz.

Unsere mobile Sicherheitstechnologie geht darüber hinaus und schützt Sie umfassend vor bösartigen und lästigen Apps. Wir verfügen über 30 Jahre Erfahrung mit IT-Sicherheit und die weltweit größte Bedrohungsdatenbank. Diese Ressourcen setzen wir ein, um Sie gegen Bedrohungen durch Android-Apps zu schützen.

Norton Mobile Insight schläft nie

Unser System Norton Mobile Insight durchsucht ständig über 200 App Stores und stellt Informationen zu Apps aus dem Norton Community Watch-Netzwerk zusammen. Alle so erfassten Daten zu Android-Apps werden anschließend mit einer Reihe zuverlässiger Tools ausgewertet, um problematische Apps zu identifizieren.

Zunächst führen wir eine statische Analyse durch. Dabei werden elementare Daten extrahiert, zum Beispiel die Bezeichnung der App, die Signatur des Entwicklers und die Liste der Berechtigungen, die gewöhnlich beim Herunterladen einer App angezeigt wird und äußerst lang sein kann.

Dann schauen wir uns den Programmcode der App genauer an, um festzustellen, welche sensiblen Anwendungsprogramm-Schnittstellen (kurz: APIs für “application program interfaces”) aufgerufen werden. So prüfen wir etwa, ob die App APIs aufruft, um Ihre Telefonnummer und andere private Informationen auszulesen und dann auf das Internet zuzugreifen. Und damit ist die Untersuchung noch nicht beendet. Wurde die App lokalisiert? Wird sie installiert, ohne dass ein Symbol auf dem Startbildschirm abgelegt wird? Die Antworten auf diese Fragen geben wichtige Hinweise zur Sicherheit der App.

Im nächsten Schritt führen wir wichtige dynamische Analysen durch, die besondere Erkenntnisse zum Datenschutz und zu Informationslecks der App liefern. Jede App wird in einem instrumentierten Android-Nachbildungsprogramm geprüft, welches ihr suggeriert, dass sie im regulären Alltagsbetrieb ausgeführt wird. Wenn eine App beispielsweise geräte- oder personenbezogene Informationen erfasst und im Hintergrund versendet, werden diese möglicherweise an unbefugte Dritte übermittelt.

Bei dieser intelligenten automatischen Analyse kommen echte Nutzungsmuster und Funktionen zum Einsatz. Viele unserer Mitbewerber stützen ihre Schlussfolgerungen zum Verhalten von Apps und ihre Risikomeldungen lediglich auf die Berechtigungen, ohne die jeweilige App tatsächlich zu testen. Dies kann jedoch dazu führen, dass die Benutzer unzutreffende Informationen und falsche Warnmeldungen erhalten.

Das sind unsere leistungsstarken Mobile Intelligence-Technologien und -Ressourcen:

Norton™ Mobile Insight ist ein dynamisches System, das ständig neue oder aktualisierte Android-Apps aus Google Play und über 200 weiteren App Stores herunterlädt und analysiert. So entsteht ein einzigartiger, fortlaufend aktualisierter Informationsbestand zu Apps. Wir untersuchen täglich über 30.000 neue Apps und haben bisher insgesamt mehr als 15 Millionen Apps analysiert.

Norton Community Watch ist eine aktive Community aus Millionen von Benutzern, die uns die Erlaubnis erteilen, anonyme Meta- und Leistungsdaten der auf ihren Android-Geräten laufenden Apps zu erfassen, von denen viele zuvor nicht bekannt waren. Norton Mobile Insight wertet die Daten aus dieser Community aus und führt Echtzeit-Analysen durch. Dies bietet eine weitere Möglichkeit, das Verhalten einer App nach der Installation zu untersuchen und einzuschätzen, welche Risiken bestehen, wenn sie sich auf dem Gerät befindet. 25 Prozent aller von Norton Mobile Insight analysierten bekannten Apps werden ausschließlich über Norton Community Watch erfasst. Wir erfahren auf diesem Weg also von vielen Apps, die nicht über App Stores verbreitet werden, und erhalten die Möglichkeit, diese zu analysieren.

Die Symantec Security Technology and Response (STAR) Division ist ein weltweites Team aus Sicherheitsingenieuren, Virenjägern, Bedrohungsanalysten und Forschern. Sie stellen die zugrunde liegende Sicherheitstechnologie, die Inhalte sowie den Support für alle Sicherheitsprodukte von Symantec bereit. Diese Experten sind unsere Augen und Ohren. Sie haben die Bedrohungslandschaft Tag und Nacht im Blick, damit Sie geschützt sind.

Je mehr Daten, desto mehr Erkenntnisse

Die Symantec Data Analytics Platform (SDAP) ist ein weiterer entscheidender Vorteil der Norton-Lösung. Sie ist als eines von wenigen Systemen leistungsstark und flexibel genug, um mit dem enormen Anstieg von Bedrohungen im Internet, im mobilen Bereich und anderswo fertig zu werden.

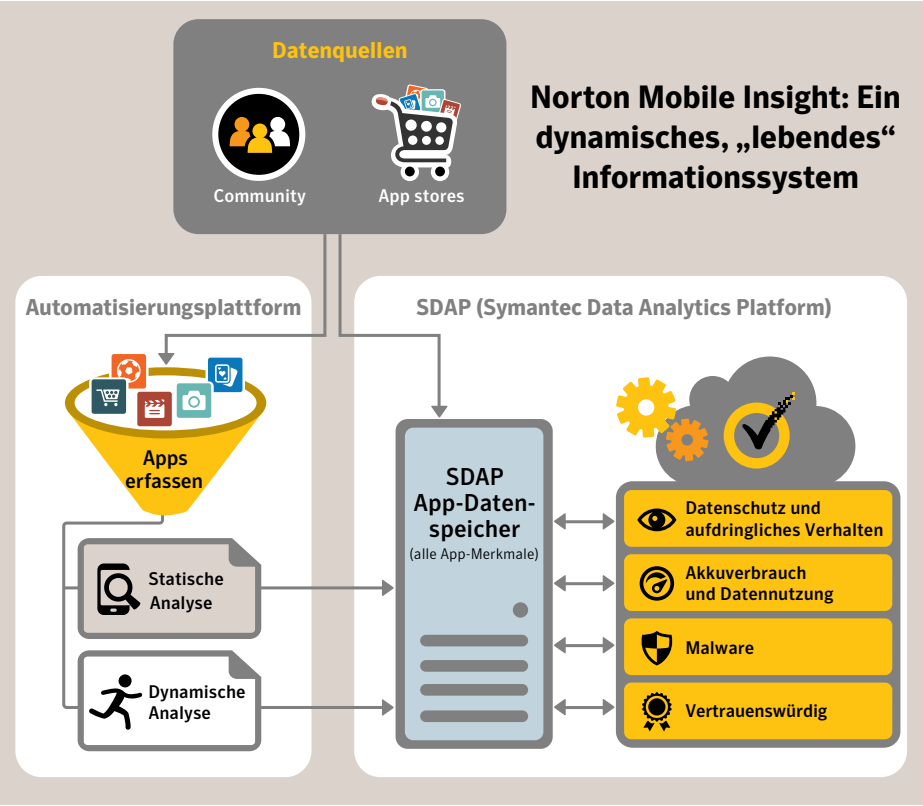
Die SDAP-Plattform ist eine riesige Datenbank, die ständig erweitert wird und alle unsere Sicherheitsdaten enthält. Allein unser Datenbestand für den mobilen Bereich umfasst rund 1,6 Billionen Einzeldaten. Das ist sehr viel – aber nur so können wir Ihr Gerät vor mobilen Bedrohungen schützen.

Alle von uns gesammelten App-Daten – vom Verhalten der Anwendung bis zur Stabilität und einzelnen Leistungsdaten – werden von der SDAP-Plattform verarbeitet. Sie geben unter anderem Aufschluss über das Leistungsverhalten der App unter Alltagsbedingungen, die Anzahl der Norton Community Watch-Benutzer, die sie verwendet haben, die App Stores, in denen sie angeboten wird und die Anzahl von Nutzern, die sie heruntergeladen haben.

Wir analysieren alle vorliegenden Daten und stellen auf dieser Grundlage fest, ob die App ist bösartig ist. Norton Mobile Insight hat bisher insgesamt mehr als 15 Millionen Apps analysiert und täglich kommen über 30.000 weitere hinzu. Es erkennt die für Malware charakteristischen Eigenschaften und Muster, prüft Apps auf Auffälligkeiten in Bezug auf Datensicherheit und Angriffe und analysiert ihren Akkuverbrauch sowie die Datennutzung.

Und mit Änderungen in der Bedrohungslandschaft gewinnt das System ständig an Intelligenz hinzu. Es lernt und entwickelt sich anhand der neu erfassten Daten. So weiß es beispielsweise, dass die Größe der eigentlichen App bei Malware eher kleiner als bei unschädlichen Apps ist, weil Malware-Entwickler in der Regel keine Zeit auf die Feinarbeit an ihren Produkten verwenden.

Norton Mobile Insight gleicht all diese Informationen anschließend mit Hunderten anderer Datenpunkte ab, um zu erkennen, ob es sich bei der betreffenden App um Malware handelt, und legt eine Vertrauensstufe für die App-Sicherheit fest. Das System identifiziert typische Anzeichen für Malware, die Angreifer nicht ohne weiteres ändern können, wie z. B. Codemuster, Techniken zur Ausführung bösartiger Verhaltensweisen und den Ruf des Entwicklers innerhalb der Community.



Heute dreht sich alles um Apps – professioneller und proaktiver Schutz ist gefragt

Norton Mobile Security ist ein leistungsstarkes webbasiertes Produkt, das Sie per Abonnement beziehen können, um sich und Ihre Mobilgeräte zu schützen. Es basiert auf der in diesem Dokument beschriebenen, professionellen Technologie Norton Mobile Insight. Norton Mobile Security spart Zeit und hilft, Apps zu erkennen, die die hier erläuterten Risiken aufweisen.

Herzstück von Norton Mobile Security ist der App-Berater – eine Funktion zum Scannen von Apps.

Die durch Norton Mobile Insight unterstützte App-Berater-Funktion bietet proaktiven Schutz. Sie ermöglicht es, Apps auf Google Play bereits VOR dem Herunterladen zu scannen (erfordert Android 4.0 oder höher bzw. für Samsung-Geräte Android 4.2 oder höher). Der App-Berater weist Sie darauf hin, wenn eine App bösartigen Code enthält oder potenzielle Datenschutzrisiken, aufdringliches Verhalten, übermäßigen Akkuverbrauch oder einen hohen Datenverbrauch aufweist. Außerdem scannt er automatisch Ihre zuvor heruntergeladenen bzw. nicht über einen App Store installierten Apps auf diese Gefahren und ermöglicht Ihnen, diese gegebenenfalls zu deinstallieren.

So können Sie sich in einem einzigen, einfachen Schritt über Android-Apps informieren und auf dieser Basis entscheiden. Sie selbst legen fest, ob eine bestimmte App Ihnen die „Kosten“ wert ist.

Norton Mobile Security bietet noch weitere proaktive Schutzkomponenten für Sie und Ihre Android-Geräte – etwa den Webschutz, der Sie gegen betrügerische Websites abschirmt, die es auf Ihre persönlichen Daten und Ihr Geld abgesehen haben. Außerdem umfasst die Lösung eine Fernortungsfunktion für Ihr Android-Gerät, iPhone und iPad, damit Sie es schnell auffinden können. Sie können sogar Ihre Kontaktinformationen speichern und bei Verlust oder Diebstahl wiederherstellen. Jetzt ist ganz einfach, Ihre verschiedenen Geräte bequem mit einem einzigen webbasierten Abonnement zu schützen. Mit Norton Mobile Security können Sie sicher von allen Möglichkeiten der mobilen Freiheit und Bequemlichkeit profitieren.

Bereit, loszulegen – mit der Lösung von Norton

Mobilität ist ein wesentlicher Bestandteil Ihres aktiven, vernetzten Lebens. Aber je mehr Sie auf Ihre Mobilgeräte – diese kleinen, handlichen Computer – angewiesen sind, desto wichtiger ist es, dass Sie die damit verbundenen Sicherheitsrisiken kennen und Maßnahmen ergreifen, um sich zu schützen.

Norton Mobile-Schutztechnologien sind ebenfalls Bestandteil unserer plattformübergreifenden Norton Security- und Norton Security mit Backup-Produktabonnements.

Mit diesen Abonnements bieten wir Ihnen und Ihrer Familie eine bedienungsfreundliche und umfassende Lösung mit maßgeschneidertem Schutz für Ihre PCs, Macs, Android- und iOS-Geräte – jederzeit und überall.

Besuchen Sie uns auf Google Play™, um alle professionellen, proaktiven Schutzmerkmale eines Norton Mobile Security Premium-Abonnements 30 Tage lang kostenlos zu testen. Sie müssen dazu lediglich einen Norton Account anlegen. Es wird keine Kreditkarte benötigt. Nach Ablauf der Testphase können Sie auf die Premium-Version upgraden oder die kostenlosen Funktionen weiterhin nutzen.