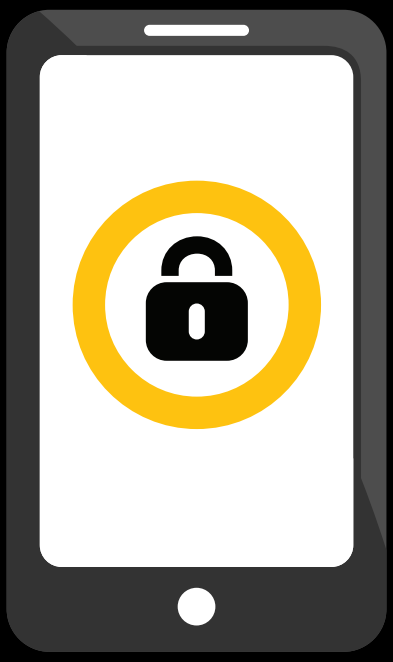
Norton by Symantec

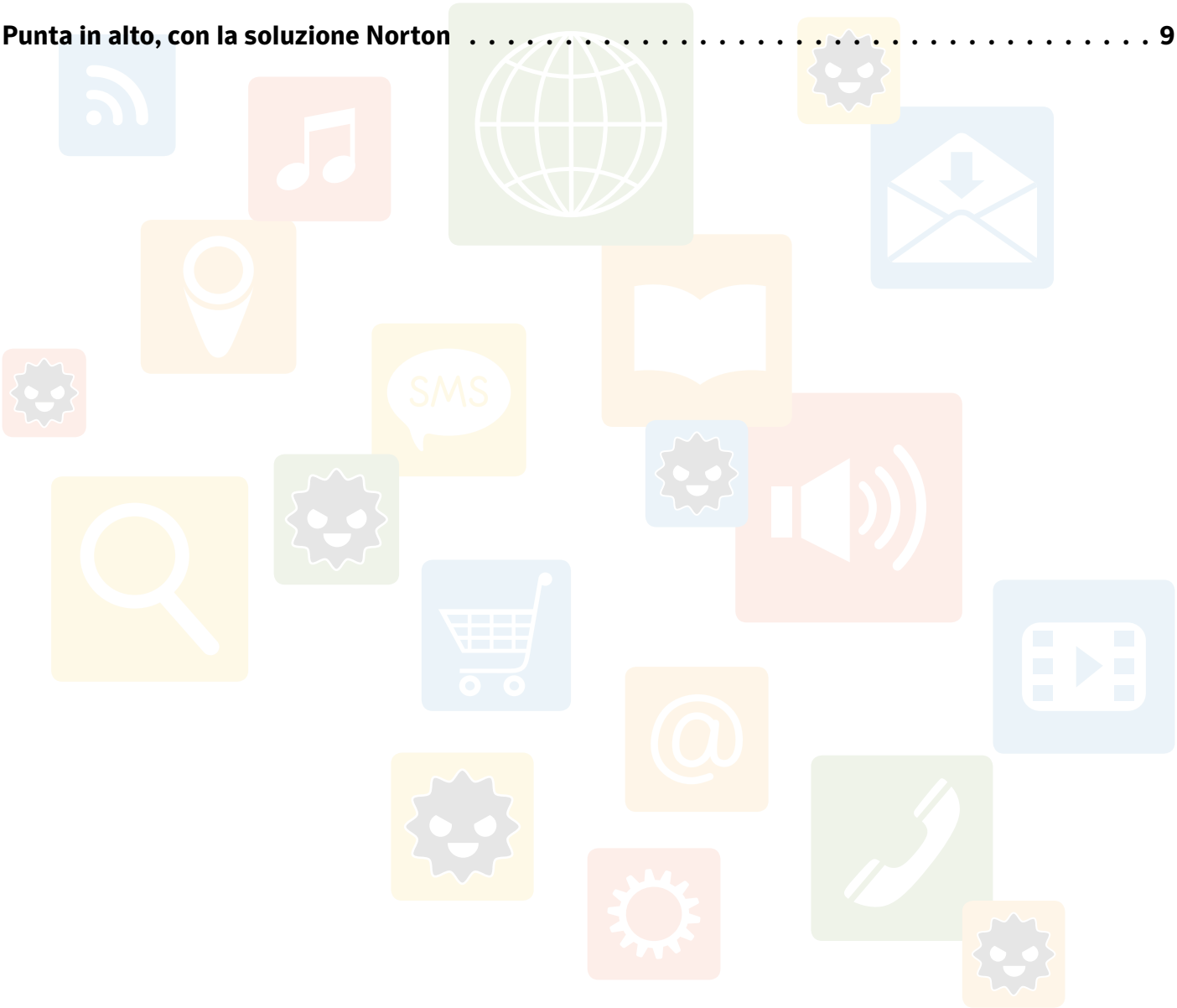
BUONE, CATTIVE O INVADENTI: SAI VERAMENTE COSA FANNO LE TUE APP?

Le app sono divertenti, utili e gratuite, ma qualche volta hanno anche costi nascosti e comportamenti nocivi. Non aspettare che ti capiti qualcosa, scegli un approcio preventivo per la protezione di tutti i tuoi dispositivi mobili.



You Tube

Indice generale



I dispositivi mobili intelligenti oggi sono diffusi ovunque. Su base globale, quasi 1,8 miliardi di persone, cioè un quarto della popolazione mondiale, possiede uno smartphone.[1] E con la crescita dei dispositivi mobili, cresce anche l'utilizzo delle app.

I possessori di smartphone in tutto il mondo oggi usano le app per l'86% del tempo e trascorrono sul Web solo il rimanente 14%.[2] Su base globale, in ogni telefono sono installate in media 26 app, che salgono a oltre 35 nei primi 10 paesi.[3]

Le app offrono tanta libertà, ti permettono di fare sul tuo dispositivo mobile le stesse cose che facevi sul PC ma in modo nuovo e diverso, avvicinandoti ogni giorno all'Internet of Things. Per esempio, già oggi puoi usare un'app per controllare la temperatura del soggiorno, accendere le luci prima di arrivare a casa e proteggere la casa dai ladri.

Con le app puoi far succedere un'infinità di cose. Se il tuo telefono è un veicolo, allora le app sono il volante, l'acceleratore e le frecce. Ma sono anche la chiave che apre la porta verso tutte le informazioni contenute nel tuo dispositivo mobile e quelle che magari salvi sul cloud.

I criminali informatici tutto questo lo sanno, e bene. Le tue informazioni personali hanno un forte valore economico e gli hacker usano tattiche sempre più collaudate e inganni realistici (come app finte e ransomware) per attaccare i dispositivi mobili.
E non sono gli unici a farlo. Anche gli sviluppatori di app più avidi sono interessati alle tue informazioni personali. I loro obiettivi non sono necessariamente illegali. Magari si limitano a inserire pubblicità mirate nella tua barra delle notifiche. Ma i metodi che usano comportano dei rischi.

Visto e considerato che le tue informazioni personali fanno gola a diversi soggetti, oggi più che mai è fondamentale sapere cosa fanno le tue app e adottare misure per mantenere protetti i tuoi dispositivi mobili.

Localizzare e bloccare un dispositivo perduto o rubato non è più sufficiente. Certo, sono pur sempre delle contromisure che aiutano a prevenire danni, ma il nuovo imperativo oggi è la sicurezza proattiva. Una protezione cioè che non ti difenda solo da app nocive volte a sottrarre soldi e dati personali, ma che ti permetta di prendere decisioni consapevoli sui rischi potenziali delle app che scarichi e di capire se quell'app gratuita vale il suo costo finale.

La protezione mobile oggi richiede un approccio moderno e preventivo, che permetta di godere liberamente e in tranquillità di tutti i vantaggi di un mondo che ruota intorno alle app.

[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/

Sai cosa fanno le tue app? Norton lo sa

La maggior parte degli utenti gestiscono le app mobili con la stessa ingenuità con cui 10 o 15 anni fa gestivano i software applicativi per PC. Installano le app mobili prestando poca o nessuna attenzione ai rischi che potrebbero derivarne. E ne installano tante, perché si scaricano con un tocco.

Le app, soprattutto quelle gratuite, comunicano con efficacia i vantaggi che ti offrono, ma non indicano quali sono i loro costi reali. Questi costi possono prendere le sembianze di minacce nascoste e altri rischi potenziali. Il sandboxing creato da Apple per il suo sistema operativo iOS, combinato con i rigidi controlli sui prodotti presenti nell'app store di iTunes, rendono improbabile l'incontro con app nocive. La natura aperta del sistema operativo Android invece, è più soggetta a manipolazioni da cui derivano minacce e potenziali rischi.

Il Symantec Internet Security Threat Report indica che nel 2013 il malware mobile è stato sviluppato quasi esclusivamente per il sistema operativo Android, con il 32% delle app che sottraggono informazioni personali dell'utente.[4]

Inoltre, più del 75% delle app mobili non è in grado di superare i test di sicurezza di base, ed evidenzia una serie di rischi e comportamenti nocivi.[5]

Infatti Symantec ha registrato una crescita del 69% delle istanze di malware mobile fra il 2012 e il 2013.[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] Dati di monitoraggio e analisi di Norton Mobile Insight/Symantec Threat and Response al dicembre 2014.

Le app nocive sono un problema reale

Perché le app mobili piacciono agli hacker è fin troppo chiaro. La base di utenti è in continua crescita e, una volta che un'app nociva è installata, la quantità di informazioni disponibili è molto significativa. Gli hacker ovviamente sono sempre più bravi, cosa che non sorprende. Imparano e condividono i loro trucchi, creando attacchi sempre più sofisticati. Di fatto, i criminali informatici hanno spostato le tattiche che hanno ben collaudato sui PC (come phishing, software fittizi e ransomware) verso i dispositivi mobili.

Ricordiamo, ad esempio, la truffa basata su un'app fittizia che offriva minuti di telefonate gratuiti dal cellulare. L'offerta era disponibile solo se un utente immetteva le proprie credenziali e la inoltrava a 10 amici. La truffa puntava a massimizzare il numero di vittime, rubando le loro credenziali e raccogliendo altri dati personali.

Un'altra app fasulla era una perfetta copia dell'app vera di Mizrahi Bank, una delle più importanti banche israeliane. Gli hacker l'hanno semplicemente caricata su Google Play e da lì è stata scaricata da ignari clienti della banca. Quando questi hanno aperto l'app e inserito le loro credenziali, l'app ha preso possesso dei loro ID utente. A quel punto l'app inviava un messaggio di errore chiedendo ai clienti di reinstallare la vera app della banca, che a quel punto funzionava correttamente. La maggior parte dei clienti non si sono neanche resi conto che i loro ID utente erano stato rubati.

Un'altra minaccia recente è Android. Simplocker, un trojan ransomware contenuto in un'app fittizia. Una volta installato sul proprio dispositivo, crittografa (o blocca) i file, quindi visualizza un finto avviso dell'FBI che sostiene di aver rilevato materiale pornografico illegale sul dispositivo. L'utente viene quindi informato che dovrà pagare una "multa" di 300 dollari attraverso il servizio di pagamento MoneyPak per sbloccare i propri file.

Guida rapida alle app nocive

Oltre il 20% dei 15 milioni di app analizzate ad oggi da Norton sono nocive.[7] Ne esistono di diversi tipi:

App basate su tracking raccolgono messaggi di testo e registri delle chiamate, tracciano le coordinate del GPS, registrano le chiamate e rubano foto e video dai dispositivi. Il Norton Report 2014 ha evidenziato come il volume delle minacce che tracciano le attività dell'utente sia cresciuto nel 2013 dal 15% al 30%.

App che rubano raccolgono dati sullo specifico dispositivo e specifico utente, ad esempio informazioni sul dispositivo, dati di configurazione e contenuti personali.

App infette eseguono funzioni malware tipiche, come installare backdoor e downloader che consentono agli hacker di accedere al dispositivo.

App che riconfigurano il sistema cambiano i diritti d'accesso o modificano le impostazioni del sistema operativo, aprendo la porta a intrusi.

App che rubano soldi sono basate sull'uso di numeri per SMS a tariffe alte con brevi codici. Con l'app, gli hacker installano un malware che invia SMS a quei numeri dai dispositivi infetti. Gli utenti ricevono l'addebito dal loro gestore e gli hacker i soldi.

App a due fattori per furto sono in grado di intercettare un messaggio di testo inviato all'utente dalla sua banca e contenente un codice di autenticazione valido una sola volta, tramite il quale gli hacker possono accedere al conto in banca dell'utente.

[7] Dati di monitoraggio e analisi di Norton Mobile Insight/Symantec Threat and Response al dicembre 2014.

Anche il grayware è un rischio

Il confine fra il software legale e il malware non è troppo ben definito. Esiste infatti una classe di app, denominate *grayware*, posizionate in un'ambigua zona di confine. In questo settore operano molti sviluppatori di app non nocive che hanno gioco facile nel persuadere gli utenti a scaricare app potenzialmente rischiose – che infatti rendono vulnerabili le loro informazioni e contenuti – usando come esca un'app "gratuita".

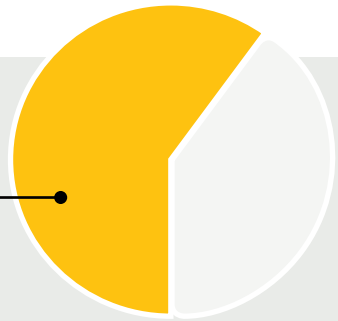
Le app grayware non contengono codice nocivo ma possono ugualmente compromettere la privacy dell'utente e colpire il dispositivo con pubblicità e altri comportamenti fastidiosi. Un tipo comune di *grayware* denominato *mobile adware*, o *madware*, include app che visualizzano annunci pubblicitari in una barra di notifica del telefono, sostituiscono la suoneria con pubblicità vocali o, peggio ancora, rendono pubblici dati privati quali il numero di telefono o le informazioni dell'account utente.

L'utente può essere in grado di accorgersi prima di questi rischi se ha una competenza tecnica di base e legge bene la lunga lista di permessi che l'app richiede quando viene scaricata da Google Play. Ma spesso le cose non vanno così. Anche leggendo con attenzione i permessi richiesti, non è dato sapere quali saranno i comportamenti effettivi dell'app.

Le indagini di Norton hanno dimostrato che oltre il

60%

delle app Android contengono adware o altro grayware.[8]



Una volta installato, il grayware può tracciare la posizione dell'utente o monitorare la sua navigazione, per vendere tali informazioni a fini di marketing. In molti casi un'app ha qualche buona scusa per raccogliere i dati sensibili dell'utente, ma questi non conosce i comportamenti dell'app e non è detto che sarebbe d'accordo all'idea di condividere certe informazioni personali con quella specifica app. Consideriamo, per esempio, il caso di un'app che rileva il numero di telefono dell'utente come ID unico dal dispositivo e lo trasmette in pubblico senza crittografarlo. D'improvviso il numero è a disposizione di chi fa marketing e di artisti delle truffe in varie parti del mondo.

Un'app, inoltre, può rappresentare un rischio potenziale per la privacy perché raccoglie informazioni non correlate alle finalità d'uso dell'app stessa. Ad esempio, perché mai un'app di previsioni meteo dovrebbe poter accedere ai contatti o al calendario?

È comune anche il caso di app che consumano molto la batteria, riducono le prestazioni del dispositivo, scaricano dati dalla rete e fanno salire i costi della bolletta. Anche se tecnicamente non si tratta di grayware, rimane comunque il fastidio. Molte agiscono di nascosto in background. Hai mai notato che con il tempo la batteria offre prestazioni gradualmente inferiori? Le tue app potrebbero essere la causa. Gli addebiti per l'uso dei dati sono improvvisamente diventati alti? Sono sempre le app, probabilmente. Molte di queste eseguono continui download anche quando non sono aperte.

[8] Dati di monitoraggio e analisi di Norton Mobile Insight/Symantec Threat and Response al dicembre 2014.

Norton garantisce la migliore protezione mobile

Norton è da sempre una scelta sicura per il tuo PC. Oggi utilizziamo le stesse tecnologie avanzate, capacità di ricerca e risorse di intelligence globale anche per proteggere il tuo dispositivo mobile.

La maggior parte degli attuali prodotti di sicurezza mobile offre solo una protezione di base.

Noi facciamo di più, offrendoti una tecnologia che garantisce protezione completa contro le app nocive e fastidiose. Grazie ai nostri 30 anni di esperienza nel settore della sicurezza e al più grande database al mondo di minacce informatiche siamo in grado di proteggerti dalle app a rischio presenti su Android.

Norton Mobile Insight non dorme mai

Tutti i dati delle app Android che raccogliamo tramite Norton Mobile Insight – monitorando costantemente oltre 200 app store e registrando tutte le informazioni sulle app provenienti dalla rete Norton Community Watch – vengono immessi nella nostra pipeline di elaborazione e passano attraverso un aggiornato set di strumenti per identificare quelle che generano problemi.

Come prima cosa, eseguiamo analisi statiche che includono l'estrazione dei dati di base come il titolo dell'app, la firma dello sviluppatore e l'elenco dei permessi richiesti – mostrati di solito quando si scarica l'app – verificando se sono troppi.

Quindi andiamo più a fondo nel codice dell'app per vedere quali interfacce di programmi applicativi (API) sensibili vengono utilizzate. Ad esempio, l'app usa delle API che leggono il numero di telefono dell'utente e altre informazioni private e quindi accedono a Internet? E le nostre domande non finiscono certo qui. Verifichiamo se l'app è localizzata. Si installa senza visualizzare un'icona nella barra di lancio? Queste informazioni sono fondamentali per valutare la sicurezza di un'app.

A questo punto passiamo alle analisi dinamiche, che ci dicono tutto sull'eventuale divulgazione di informazioni e dati personali dell'utente che l'app può generare. Eseguiamo ogni app in un simulatore di Android dotato di strumenti che dà all'app la sensazione di operare nel mondo reale. Per esempio, se l'app raccoglie e invia al di fuori del dispositivo informazioni personali o del dispositivo stesso agendo in background, tali informazioni potrebbero essere dirette a terzi.

Eseguiamo queste analisi in modo intelligente e automatizzato, riproducendo flussi e caratteristiche d'uso del mondo reale. Molti dei nostri concorrenti si limitano a dedurre i comportamenti delle app mobili e indicare i rischi in base ai permessi richiesti dalle app senza effettuare tuttavia i test, ottenendo così informazioni poco accurate o generando falsi allarmi presso gli utenti.

Le nostre tecnologie e risorse esclusive di intelligence mobile comprendono:

Norton™ Mobile Insight è un sistema dinamico che scarica e analizza costantemente app Android nuove o aggiornate da oltre 200 app store, fra cui Google Play, creando un eccezionale sistema di intelligence sulle app in continuo aggiornamento. Analizziamo oltre 30.000 nuove app al giorno, con oltre 15 milioni di app analizzate a oggi.

Norton Community Watch è una rete attivissima composta da milioni di utenti che ci consentono di raccogliere in modo anonimo metadati e dati sulle prestazioni dalle app che eseguono sui loro dispositivi Android, fra cui molti file di app mai elaborati in precedenza. Utilizzando i dati di questa grande comunità ed eseguendo analisi in tempo reale, Norton Mobile Insight ha a disposizione un ulteriore strumento per comprendere i comportamenti delle app una volta che vengono installate, e quali rischi si corrono ad averle sul proprio dispositivo. Di fatto, il 25% delle app note che vengono analizzate da Norton Mobile Insight provengono da Norton Community Watch, il che significa che analizziamo e studiamo moltissime app non distribuite tramite i normali app store.

Symantec Security Technology and Response (STAR) è una divisione composta da un team mondiale di ingegneri addetti alla sicurezza, cacciatori di virus, analisti di minacce e ricercatori che forniscono le tecnologie di sicurezza, i contenuti e il supporto di tutti i prodotti di sicurezza Symantec, compresi quelli mobili. Questi esperti sono i nostri occhi e le nostre orecchie, sorvegliano giorno e notte lo scenario delle minacce per la tranquillità di tutti.

Dati: più ne hai, più sai

La soluzione Norton offre i grandi vantaggi di Symantec Data Analytics Platform (SDAP), uno dei pochi sistemi abbastanza potenti e agili da tenere testa all'enorme crescita di minacce informatiche, nel settore mobile e non solo.

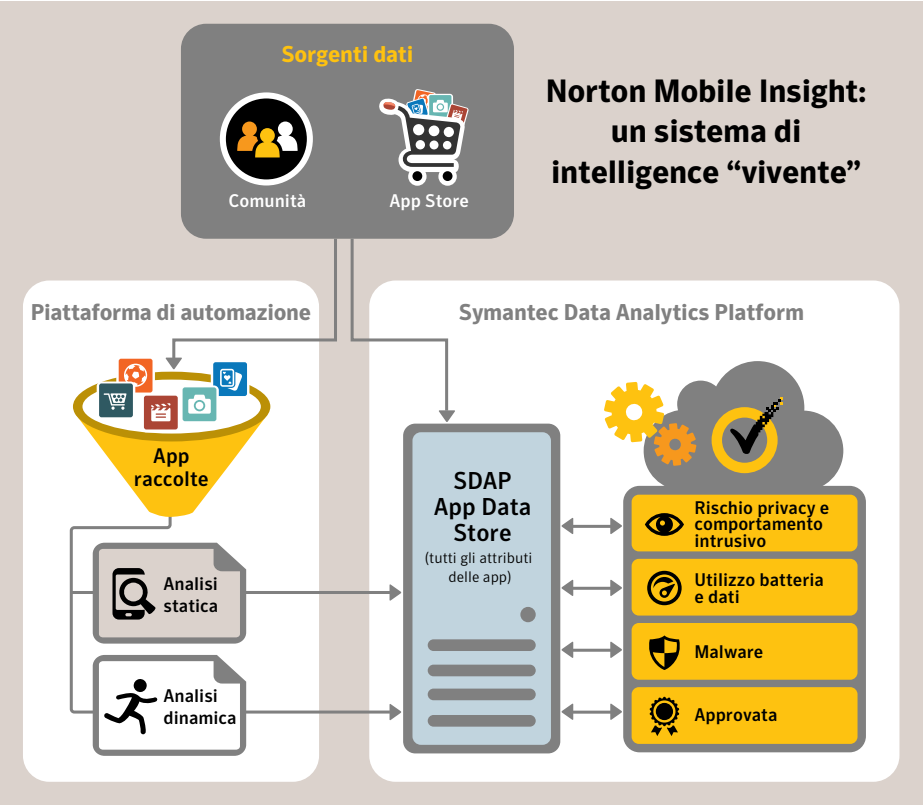
La piattaforma SDAP è un gigantesco database in continua espansione che ospita tutti i nostri dati sulla sicurezza. I nostri dati mobili sono circa 1.600 miliardi di singoli elementi di dati, un'infinità di informazioni. Ma è questo che serve per garantire protezione al tuo dispositivo dalle minacce mobili.

Tutti i dati sulle app che raccogliamo – dai comportamenti delle applicazioni alla loro stabilità fino ai dettagli sulle prestazioni – vengono elaborati dalla piattaforma SDAP. Questi dati comprendono informazioni sulle prestazioni delle app nel mondo reale, quante persone della Norton Community Watch le hanno usate, in quali app store si trovano e quante persone le hanno scaricate.

Analizziamo tutti questi dati e in base a ciò stabiliamo se l'app è nociva o meno. Norton Mobile Insight ha elaborato a oggi oltre 15 milioni di app e ogni giorno ne elabora altre 30.000 nuove. Rileva le funzionalità e gli schemi d'uso che indicano la presenza di malware, controlla se le app operano in modo sospetto per la privacy o se hanno comportamenti intrusivi ed esamina l'uso che fanno della batteria e dei dati.

L'intelligence di Norton Mobile Insight si affina di giorno in giorno, seguendo l'evoluzione delle minacce. Il sistema impara e si sviluppa sulla base dei nuovi dati che acquisisce. Ad esempio, sa che le dimensioni delle app che contengono malware sono limitate rispetto alle app non nocive, perché i loro sviluppatori non hanno grande interesse a strutturarle in modo completo.

Norton Mobile Insight incrocia quindi le informazioni in suo possesso con centinaia di altri dati per verificare se l'app è di fatto un malware e imposta il livello di sicurezza della specifica app. Il sistema riconosce gli elementi intrinseci del malware che un criminal e informatico non può facilmente modificare, come certi schemi del codice, le tecniche per eseguire comportamenti nocivi e la stessa reputazione dello sviluppatore nella comunità.



La protezione proattiva avanzata che serve per godersi i vantaggi delle app

Norton Mobile Security è un efficace abbonamento basato sul Web che protegge te e i tuoi dispositivi mobili. Utilizza l'avanzata tecnologia Norton Mobile Insight illustrata nel presente documento. Norton Mobile Security è stato pensato per farti risparmiare tempo e non costringerti a studiare ogni singola app per identificarne gli eventuali rischi, come spiegato qui.

Il punto centrale di Norton Mobile Security è una funzionalità di scansione delle app denominata Analisi App.

Grazie alla tecnologia Norton Mobile Insight, la funzione Analisi App ti garantisce protezione proattiva consentendoti di scansionare automaticamente le app su Google Play PRIMA di scaricarle (su Android 4.0 o versioni successive o su Android 4.2 o versioni successive su dispositivi Samsung). Il sistema ti avverte se un'app contiene codice nocivo, comporta rischi per la privacy, manifesta comportamenti intrusivi o richiede un elevato utilizzo della batteria o dei dati. Il sistema inoltre scansiona automaticamente le app Android scaricate in precedenza o le app installate al di fuori degli app store per individuare la presenza degli stessi rischi e consentirti di rimuoverle se lo desideri.

In un unico passaggio puoi prendere sempre la decisione giusta sulle app per Android. Puoi decidere se una determinata app vale il suo "costo."

Norton Mobile Security ti offre inoltre altri componenti di sicurezza proattiva per te e i tuoi dispositivi Android, come la Protezione Web per proteggerti da siti Web fraudolenti creati per rubare informazioni personali e soldi. Il sistema offre inoltre il recupero del dispositivo da remoto per dispositivi Android, iPhone e iPad, per aiutarti a ritrovarli presto. Puoi salvare le informazioni sui contatti e ripristinarle in caso di smarrimento o furto. Ora puoi facilmente proteggere tutti i tuoi dispositivi con un unico servizio in abbonamento basato sul Web. Norton Mobile Security consente di sfruttare a pieno lo straordinario potenziale di libertà e praticità dell'universo mobile, in tutta sicurezza.

Punta in alto, con la soluzione Norton

La mobilità è un aspetto irrinunciabile per restare connessi e mantenere i propri impegni. Ma fare affidamento su questi piccoli computer – cioè sui tuoi dispositivi mobili – significa saper riconoscere subito i rischi per la sicurezza mobile e adottare le giuste misure di protezione.

Le tecnologie di protezione Norton Mobile sono disponibili anche tramite i nostri abbonamenti multipiattaforma Norton Security e Norton Security con Backup.

Questi abbonamenti garantiscono a te, alla tua famiglia e alla tua attività la protezione su misura richiesta per i tuoi PC, Mac, dispositivi Android e iOS con un'unica soluzione facile da usare e disponibile in qualunque momento e luogo.

Visitaci su Google Play™ per provare le funzionalità della protezione proattiva e avanzata dell'abbonamento a Norton Mobile Security Premium gratis per 30 giorni. È sufficiente creare un account Norton, per il quale non serve la carta di credito. Una volta terminato il periodo di prova, puoi fare l'upgrade alla versione Premium o continuare a utilizzare le funzionalità gratuite.