



Ikmēneša Informācijas drošības izdevums tev

Droša mobilo lietotņu izmantošana

Pārskats

Tādas mobilās ierīces kā planšētdatori, viedtelefonu un viedpulksteņi kļuvuši par vienām no biežāk izmantotajām tehnoloģijām, kuras lietojam gan privātajā, gan darba dzīvē. Šīs ierīces tik populāras padara tieši milzīgais pieejamo lietotņu klāsts. Lietotnes palīdz mums kļūt produktīvākiem, komunicēt ar citiem un dalīties ar informāciju, organizēt apmācības un izglīties pašiem vai vienkārši izklaidēties. Lūk, daži soļi, kurus vari spert, lai šodien pieejamo lietotņu izmantošana būtu droša un sniegtu labāko efektu.

legūsti drošas mobilās lietotnes

Kibernoziedznieki attīstījuši prasmes šķietami īstu viltus lietotņu izveidē un izplatīšanā ļaunprātīgos nolūkos. Bieži, instalējot kādu no šīm lietotnēm, tu dod noziedzniekiem iespēju pārņemt pilnīgu kontroli pār tavu ierīci vai datiem. Šī iemesla dēļ jābūt pārliecinātam, ka lejupielādē tikai drošas mobilās lietotnes no uzticamiem avotiem. Iespējams, tu neaptver, ka to, kādas lietotnes tev pieejamas, nosaka tas, kāda ražotāja mobilo telefonu lieto.

Apple ierīcēm lejupielādei pieejamas tikai lietotnes no Apple App Store. Priekšrocības rada tas, ka Apple veic visu mobilo lietotņu drošuma pārbaudi, pirms padara tās pieejamas klientiem. Lai gan Apple nevar atpazīt visas ļaunprātīgi izveidotās lietotnes, tomēr šāda vides uzraudzība ievērojami mazina iespēju lejupielādēt tāda veida lietotnes. Turklāt, ja Apple uziet kādu lietotni, kuru uzskata par ļaunprātīgi izveidotu, piekļuve tai operatīvi tiek liegta.

Android ierīcēm lejupielādei pieejamas mobilās lietotnes tikai no Google Play, kura uzturētājs ir Google. Līdzīgi kā Apple, Google veic visu mobilo lietotņu drošuma pārbaudi, pirms padara tās pieejamas klientiem. Android ierīces atšķiras ar to, ka vari iespējot atsevišķas opcijas, kas ļauj lejupielādēt mobilās lietotnes no citiem avotiem. Mēs silti iesakām tā nerīkoties, jo tādā gadījumā jebkurš, tai skaitā kibernetiķi, var netraucēti radīt un izplatīt ļaunprātīgos nolūkos izstrādātas lietotnes un apmānīt tevi, inficējot tavu mobilo ierīci.

Neatkarīgi no tā, kāda ražotāja ierīces izmanto, pirms aplikācijas lejupielādes veic tās izpēti. Pievērs uzmanību tam, cik ilgi mobilā lietotne bijusi pieejama, cik lietotāju tai ir un kas to pārdod.

Jo ilgāk lietotne bijusi publiski pieejama, jo vairāk cilvēku būs to izmēģinājuši un atstājuši pozitīvus komentārus un jo biežāk lietotnes pārdevējs veicis tās atjaunināšanu, jo lielāka ir iespēja, ka šī lietotne ir uzticama. Uzstādi ierīcē tikai tādas lietotnes, kuras tev vajadzīgas un kuras izmanto.

Pajautā sev: „Vai man šī lietotne tiešām vajadzīga?” Līdz ar katras lietotnes uzstādīšanu palielinās ne tikai potenciālā kaitniecības iespēja, bet rodas arī jauni ar privātumu saistīti riska faktori. Ja pārtrauc izmantot kādu lietotni vai tā zaudējusi savu lietderīgumu, izdzēs to no savas mobilās ierīces (vienmēr pastāvēs iespēja to uzstādīt no jauna, ja sapratīsi, ka tas nepieciešams).

Lietotņu privātums un atļaujas

Kad esi lietotni uzstādījis, pārliecinies, vai tā aizsargā tavu privātumu. Vai šai lietotnei tiešām ir nepieciešama piekļuve jūsu atrašanās vietai, mikrofonam vai kontaktpersonām? Sniedzot lietotnei kādas atļaujas, pastāv iespēja, ka atļauj tās izstrādātājiem tevi izsekot un pat dalīties ar informāciju par tevi vai pārdot to citiem. Ja nevēlies sniegt šāda veida atļaujas, vienkārši atsaki atļauju pieprasījumus, ļauj lietotnei piekļūt tavai informācijai tikai tās izmantošanas laikā vai atrod citu lietotni, kas atbilst tavām prasībām. Atceries, ka izvēles iespējas ir ļoti plašas.

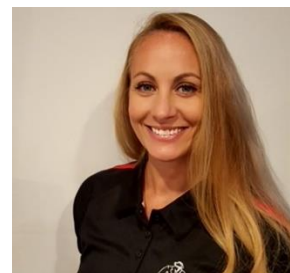
Lietotņu atjaunināšana

Gluži kā tava datora un mobilās ierīces operētājsistēmai, arī mobilajām lietotnēm vajadzīga atjaunināšana. Noziedznieki arvien meklē un atrod jaunas vājās vietas dažādās lietotnēs un rada jaunus veidus, kā šīs vājās vietas izmantot savā labā. Lietotņu izstrādātāji rada un izplata atjauninājumus, lai novērstu šīs vājās vietas un aizsargātu tavas ierīces. Jo biežāk pārbaudi atjauninājumu pieejamību un uzstādi tos, jo labāk. Lielākā daļa ierīču ļauj sistēmā iestatīt automātisku mobilo lietotņu atjaunināšanu. Silti iesakām iespējot šos iestatījumus.

Mobilās lietotnes nodrošina tev iespēju savas ierīces izmantot pēc iespējas pilnvērtīgāk. Nepieciešams vien uzmanīties, pievēršot uzmanību tam, kādas lietotnes izvēlies, un tam, kā lietot tās pēc iespējas drošākā veidā.

Viesredaktors

Domenika Kronjale (*Domenica Crognale*) ir kvalitātes nodrošināšanas inženiere un sertificēta SANS institūta instruktore. Viņa ir FOR585 : Viedtālrunu padziļinātā analīze (Smartphone Analysis In-Depth) līdzautore. Sazinies ar Domeniku *Twitter* platformā [@domenicacrognal](https://twitter.com/domenicacrognal).



Resursi

Atjauninājumu nozīme: <https://www.sans.org/newsletters/ouch/the-power-of-updating/>

Privātums: <https://www.sans.org/newsletters/ouch/privacy/>

Tulkojums: CERT.LV

OUCH! izdod SANS institūts programmas “Security Awareness” ietvaros un tas tiek izplatīts saskaņā ar [Creative Commons BY-NC-ND 4.0 licences nosacījumiem](https://creativecommons.org/licenses/by-nc-nd/4.0/). Jūs varat brīvi dalīties ar šo biļetenu vai izplatīt, kamēr jūs to nepārdodat un nepārveidojat. Redakcijas kolēģija Valters Skrivenšs (Walter Scrivens), Fils Hofmans (Phil Hoffman), Alans Vagoners (Alan Waggoner), Leslija Ridauta (Leslie Ridout), Princesa Janga (Princess Young).