**Pranešimas žiniasklaidai**

2021 m. liepos 28 d.

**Siunčiatės naują programėlę: pasitikrinkite, ar nekeliate sau pavojaus?**

**Taip lengviau: greitasis skaitymas**

|  |
| --- |
| * **Kenkėjiškos programėlės gali lėtinti telefono veikimą, lemti greičiau išsikraunančią bateriją ar net kelti grėsmę jūsų duomenų saugumui** * **Programėles siųskitės tik iš oficialių parduotuvių – „Google Play“ arba „App Store“** * **Nedidelis skaičius teigiamų ir vienodu stiliumi parašytų atsiliepimų – signalas, kad programėlė gali būti kenkėjiška** * **Suteikite programėlėms tik tuos leidimus, kurie yra būtini tiesioginėms funkcijoms atlikti** |

**Pandemijos metu augo kenkėjiškų programėlių skaičius: „Google“ pernai iš savo programėlių parduotuvės ištrynė beveik milijoną – net 962 tūkst. produktų. Tai yra net 20 proc. daugiau nei užpernai, rodo „Google“ duomenys. Kenkėjiškos programėlės gali sulėtinti telefono veikimą, lemti greitai išsikraunančią bateriją ar net visai sugadinti išmanųjį įrenginį. Kaip apsisaugoti, pranešime žiniasklaidai pataria „Bitės Profai“.**

„Kenkėjiškos programėlės gali kelti grėsmę ir jūsų duomenų saugumui: nutekinti banko kortelės ir asmeninius duomenis, nuotraukas bei slapta siuntinėti SMS žinutes padidinto tarifo numeriais. Svarbiausia, kad programėlės veikia nepastebimai, tad net neįtarsite, kad tapote auka. Norint išvengti tokių nemalonumų, prieš siunčiantis programėlę, būtina atlikti namų darbus“, – sako „Bitės Profas“ Martynas Vrubliauskas.

1. **Patikrinkite programėlės adresą**

Pirmasis pavojaus signalas, nurodantis, kad programėlė gali būti nepatikima, yra keistas jos atsisiuntimo adresas.

„Tiesiausias kelias į kenkėjiškas programėles – per įtartinuose interneto puslapiuose, nežinomų siuntėjų laiškuose ar SMS žinutėse patalpintas nuorodas. Jei radote patinkančią programėlę, kuri iš pirmo žvilgsnio atrodo saugi, tačiau jos nėra oficialiose parduotuvėse – „Google Play“ arba „App Store“ – nesisiųskite jos“, – pataria „Bitės“ išmaniųjų įrenginių ekspertas.

1. **Perskaitykite atsilepimus**

Antras žingsnis prieš atsisiunčiant naują programėlę – įvertinti vartotojų komentarus.

„Vartotojų atsiliepimai – vienas svarbiausių indikatorių, kad programėlė gali būti kenksminga. Jei daug žmonių skundžiasi, kad nuolat iššoka įkyrios reklamos ar produktas stringa, geriausia ieškoti kitos. O kai po programėle mažai komentarų ar jie netaisyklingi bei neinformatyvūs, paieškokite informacijos „Google“. Ten tikrai turėtumėte rasti atsakymą, ar susidūrėte su apgaulinga programėle“, – tikina M. Vrubliauskas.

1. **Įvertinkite kūrėjų patikimumą**

Ekspertas pasakoja, kad įvertinti programėlės kūrėjų patikimumą leidžia patys telefonai. „Android“ telefonuose esantis įrankis „Google Play Protect“ tikrina programėles iškart po to, kai jas įdiegiate. Radęs grėsmių, atsiunčia pranešimą, kad pašalintumėte programą ar net tą padaro automatiškai. Tokiu atveju gausite pranešimą, kad programa pašalinta.

„Samsung“ telefonuose šią užduotį papildomai gali atlikti ir gamintojo įdiegta apsauga, kurią aktyvuosite atvėrę nustatymus, spustelėję „Akum. ir įrenginio priežiūra“ ir „Įrenginio apsauga“. O „Xiaomi“ įrenginiuose programėlės automatiškai patikrinamos po kiekvieno naujo įdiegimo, taip apsaugant jūsų įrenginį nuo grėsmių.

1. **Nesuteikite nepasvertų leidimų**

Išvengti nemalonumų padės ir kritinis įvertinimas, ar leidimai, kurių reikalauja diegiama programėlė, yra būtini sklandžiam jos darbui užtikrinti.

„Atverdami naują programėlę, būsite paprašyti suteikti leidimus naudoti telefone esančią informaciją. Šis žingsnis būtinas tam, kad ji galėtų vykdyti savo tiesiogines funkcijas. Rekomenduoju visuomet kritiškai įvertinti, ar programėlei einamuoju momentu reikalingas prašomas leidimas ir suteikti jį tik vienam kartui. Na, nebent visiškai pasitikite programėle, pavyzdžiui, interneto banko „Swedbank“ programėle“, – tikina „Bitės Profas“.

Ekspertas priduria, kad niekuomet nepatvirtintumėte staiga telefono ekrane iššokusių leidimų pranešimų, kai programėlė nėra paleista. Tai – signalas, kad susidūrėte su programomis, galinčiomis sugadinti ar sunaikinti telefone esančius duomenis – Trojos arkliais.

1. **Pavojaus signalas – sutrikusios funkcijos**

M. Vrubliausko teigimu, gali būti, kad net ir laikantis visų šių patarimų, vis tiek parsisiųsite kenkėjišką programėlę. Tą suprasite iš sutrikusio telefono veikimo.

„Įsidiegus kenkėjišką programėlę, jūsų telefonas turėtų pradėti veikti kur kas lėčiau nei įprastai. Taip pat Trojos arklių užduočių vykdymas gali labai greitai išeikvoti baterijos energiją bei sutrikdyti gamintojo programėlių vykdymą. Tad pastebėję šiuos ar kitus staigius pokyčius, skubiai pašalinkite įtarimų keliančias programėles“, – perspėja „Bitės Profas“.

M. Vrubliauskas nurodo, kad užkrėstų programėlių sąraše šiandien galima rasti „Auxiliary Message“, „Fast Magic SMS“, „Free CamScanner“, „Travel Wallpapers“ ir primygtinai rekomenduoja jų nesisiųsti.

Daugiau apie tai, kaip atpažinti, ar išmanioji programėlė yra saugi, galite sužinoti iš didžiųjų miestų „Bitės“ salonuose įsikūrusių „Bitės Profų“. Išmaniųjų technologijų ekspertai konsultuoja nemokamai nepriklausomai nuo to, kokio tinklo paslaugomis naudojatės. Daugiau naudingų patarimų ir įdomių naujienų ieškokite „Bitės Profų“ puslapyje <https://www.bite.lt/profai>.

Daugiau informacijos:

Jaunius Špakauskas

„Bitė Lietuva“ Korporatyvinės komunikacijos vadovas

+370 682 66188, Jaunius.Spakauskas@bite.lt