Technologijų dėka mūsų gyvenimas kiekvieną dieną tampa lengvesnis ir paprastesnis. Šiandien išties nesudėtinga naudojantis telefonu atsisiųsti visą tuziną skirtingų programėlių, naršyti internete ar pramogauti. Nelaimei, gyvenimas paprastėja ir piktavaliams, kurie, naudodamiesi telefoniniais virusais, nori pakenkti kitiems. Tačiau yra ir dvi geros žinios. Viena ta, kad yra ne vienas būdas atpažinti telefoninį virusą šiam dar nepatekus į telefoną. Kita – „Bitės Profai“, kurie dalinasi realiais patarimais, kaip laiku atpažinti telefoninius virusus ir išvengti jų „malonės“.

„Tenka pastebėti, kad žmonės dažniausiai kreipiasi su klausimais, ką daryti, kai telefone „apsigyvena“ virusas. Tačiau norisi priminti galimybę išvengti virusų šiems dar nepatekus į telefoną. Viskas, ko reikia – žinoti rizikingiausias situacijas bei pasistengti jų išvengti“, – sako „Bitės Profas“ Andrius Archangelskis, dirbantis Alytaus „Bitės“ salone ir dalinasi išskiria įtartinas situacijas, kai mūsų telefonui gresia didžiausias pavojus. .

Įtariamasis nr. 1 – „Download“ mygtukas

„Dažniausiai nepatariame programėlių ieškoti patiems internete, o siųstis jas iš oficialių „App Store“ ar „Play Store“ parduotuvių. Bet jei jau leidžiatės į savarankiškas programėlių paieškas interneto platybėse, reikėtų šiukštu vengti puslapių, kuriuose prieš akis iššoka daugiau nei vienas „Download“ ar panašūs mygtukai. Tokiais puslapiais siekiama supainioti žmogų. Jis, nežinodamas, kurį tiksliai mygtuką spausti, bando spausti visus, o po šiais mygtukais dažniausiai slepiasi virusai ar kitokios kenkėjiškos programos. Tad kai tik pamatote tokią svetainę, geriau ją iškart išjungti ir niekur nespausti. Tiesa, tokių svetainių šiandien sparčiai mažėja, bet jų vis dar pasitaiko naršant internete“, – teigia A. Archangelskis.

Įtariamasis nr. 2 – vartotojų komentarai ir „Google“ testas

Pasak A. Archangelskio, vartotojų komentarai po programėlėmis – geriausias jų veidrodis: „Geras įprotis, kurį naudojantis telefonu visuomet skatiname – skaityti kitų vartotojų atsiliepimus. Ypatingai po įvairiomis programėlėmis. Taip, šis skaitymas dažnai kainuos bent kelias papildomas minutes, tačiau jos tikrai atsiperka. Tokie komentarai gali būti vienas pirmųjų indikatorių, kad su programėle ne viskas tvarkoje. Jei didelė dalis kitų vartotojų skundžiasi apie nuolat iššokančias reklamas ar pabrėžia, kad programėlė neveikia taip, kaip turėtų, tokią programėlę geriausia ignoruoti ir ieškoti kitos. O jeigu po programėle komentarų mažai arba jie įtartini – netaisyklingai parašyti, neinformatyvus – visada patariame apie konkrečią programėlę informacijos paieškoti „Google“. Jei ne vartotojų komentarai, tuomet dažnai ylai iš maišo išlįsti padeda atsiliepimai „Google“.

Įtariamasis nr. 3 – jungtis su kompiuteriu

„Jeigu reikia prijungti savo telefoną USB jungtimi prie asmeninių kompiuterių, o ypač tų, kuriais naudojasi daug žmonių, verta pasitikrinti, ar kompiuteryje nėra virusų. Nes jei kompiuteryje krebžda virusai, netgi mažiau kenksmingi, didelė tikimybė, kad USB jungtimi jie pateks ir į telefoną. Ypatingai tais atvejais, kai telefonas nėra papildomai apsaugotas. Laimei, yra puikių antivirusinių programėlių, skirtų mobiliesiems telefonams, kurios skenuoja ne tik tai, kas yra pačiame telefone, bet ir USB jungtimis perduodamą informaciją. Dauguma naujausių „Android“ telefonų turi jau gamintojų įdiegtas antivirusines programėles. Jas galima rasti įrenginio priežiūros meniu skiltyje, tik reikia patikrinti, ar ši programėlė yra įgalinta veikti. Jei ne – reikėtų įgalinti. O jei telefone nėra gamintojo įdiegtų antivirusinių programėlių, rekomenduoju rinktis „AVG“, „Malwarebytes“ ar „Kaspersky mobile antivirus“, – pataria ekspertas.

Įtariamasis nr. 4 – keistos žinutės, pranešimai ar laiškai

A. Archangelskis perspėja ir tuos, kurie telefonu naudojasi vien tam, kad skambintų, skaitytų SMS žinutes ar el. laiškus: „Tikriausiai nėra žmogaus, kuris į savo išmanųjį telefoną nebūtų gavęs SMS žinutės ar el. laiško su keistomis nuorodomis. Žinoma, tai – virusai. Daugelis jau puikiai identifikuoja tokius laiškus ar SMS žinutes, todėl iš karto juos ištrina ir sėkmingai išvengia viruso. Tačiau kartais pamirštama, kad jei tokius virusus pasigauna jūsų draugai ar pažįstami, įtartinų SMS žinučių ar el. laiškų galite sulaukti ir iš jų. Tuomet sunku neapsigauti – kai žinutę ar laišką atsiunčia geras bičiulis, kartais imi ir paspaudi ant nuorodos net nesusimąstęs. Todėl kai sulaukiate keisto turinio žinutės ar įtartinos nuorodos – net jei siuntėjas jums pažįstamas – niekada neskubėkite spausti ant jos.“

Įtariamasis nr. 5 – „Bluetooth“ ryšys

„Technologijos tuo ir žavi, kad leidžia patogiau ir lengviau bendrauti, keistis informacija ar tiesiog atlikti kasdienius darbus. Ta liudija ir jau dvidešimtmetį gyvuojanti „Bluetooth“ technologija, kurios dėka šiandien galime lengvai tarpusavyje sujungti skirtingus įrenginius, persiųsti failus tarp įrenginių ir kt. Tačiau lygiai taip pat lengvai šiandien šios technologijos dėka tarp įrenginių galima persiųsti ir virusus. Todėl būnant viešose erdvėse, kur aplinkui daug išmaniųjų įrenginių, verta prisiminti šią grėsmę. O prisiminus – arba pasirūpinti antivirusinėmis programėlėmis, arba iš anksto apriboti „Bluetooth“ ryšį savo įrenginiuose“, – nurodo A. Archangelskis.

Galiausiai, kaip teigia A. Archangelskis, turint daugiau klausimų apie telefoninius virusus arba norint papildomai nuo jų apsisaugoti, visada galima kreiptis į didžiuosiuose Lietuvos

miestuose įsikūrusius „Bitės Profus“, kurie bet kada patars bei atsakys į rūpimus klausimus.