REKOMENDACIJA

ASMENS DUOMENŲ APSAUGA „ANDROID“ ĮRENGINIUOSE

2015 m.

Įvadas

Valstybinė duomenų apsaugos inspekcija skiria šią rekomendaciją išmaniųjų telefonų ir planšetinių kompiuterių su „Android“ operacine sistema (toliau – OS) naudotojams. Šios rekomendacijos tikslas – padėti vartotojams suprasti, kaip apsaugoti savo asmens duomenis ir užtikrinti ryšio konfidencialumą naudojant šiuos įrenginius.

Išmanusis telefonas arba planšetinis kompiuteris – nesvarbu, ar tai būtų įrenginys su „Android“, „Microsoft“ ar kito gamintojo OS, iš esmės tai yra kompiuteris, kuriam turėtų būti taikomi visi saugumo reikalavimai, kurie taikomi bet kuriam kompiuteriui.

Kas yra asmens duomenys?

Asmens duomenys – tai vardas, pavardė, el. pašto prisijungimo duomenys, el. pašto turinys, telefono ir pašto knygelės abonentai (abonentų vardai, pavardės, gimimo datos, darbovietės, telefonai ir kt.), kalendorius, užrašinės duomenys ir t. t. Asmens duomenys – tai bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis.

Kodėl kažkas nori pavogti Jūsų duomenis?

Asmens duomenys beveik visuomet vagiami **siekiant gauti pinigų.** Kiekvienas veikiantis el. pašto adresas, rastos dokumentų nuotraukos ir skenuotos jų kopijos greičiausiai bus parduoti juodojoje rinkoje arba panaudoti siekiant gauti naudos vykdant nusikaltimą.

Nusikaltėliai, įsibrovęs į Jūsų pašto dėžutę, gali panaudoti informaciją apie Jūsų finansines operacijas ir bandyti gauti prieigą prie finansų valdymo priemonių (pvz., internetinės bankininkystės, „Paypal“ ir t. t.). Jie gali suklasifikuoti ir parduoti informaciją apie Jūsų apsipirkimo ir naršymo įpročius.

Nusikaltėliai gali pabandyti užsidirbti naudodami tiesioginį sukčiavimą, pvz., Jūsų socialinių tinklų paskyrose („Facebook“, „Twitter“, „Odnoklasniki.ru“ ir t. t.) paprašyti Jūsų draugų ir giminių pervesti pinigų.

Turite įsisąmoninti, kad yra daugybė būdų pasipelnyti, gavus prieigą prie įvairių Jūsų duomenų (atsiskaitymai už paslaugas, atsiskaitymas už automobilio stovėjimą, apsipirkimas el. parduotuvėse, virtualių valiutų pirkimai ir t**. t.), o Jūs sužinosite (galbūt!) apie duomenų vagystę paskutinis.**

Bendrieji duomenų saugumo principai

„Android“ yra gana saugi OS, bet ji visada turės vieną nepatikimą, silpniausią sistemos grandį – įrenginio vartotoją, t. y. Jus.

Todėl, šnekant apie saugumą, reikia pabrėžti, kad daugeliu duomenų vagystės atvejų yra kaltas pats vartotojas – dėl savo neatidumo, neapsižiūrėjimo arba tiesiog tingumo.

Paprasti ir nesunkiai suprantami bendrieji saugumo principai, kurie Jums, kaip vartotojui, gali padėti apsaugoti duomenis nuo vagysčių:

1. Būkite ypač atsargūs, net paranojiški. Net jei nieko nesuprantate apie kompiuterius, atsargumas neleis Jums atsipalaiduoti ir nekreipti dėmesio į akivaizdžius dalykus.
2. Nepasitikėkite niekuo, kas žada pagerinti, pagreitinti, paspartinti Jūsų turimą įrenginį – didelė tikimybė, kad tai pažeis Jūsų įrenginio saugumą[1].
3. Reguliariai darykite duomenų kopijas. Tai sumažins žalą, kurią galite patirti.
4. Reguliariai atnaujinkite savo įrenginio OS PĮ[2].

Ką reikia žinoti naudojant telefoną su „Android“ OS?

Android“ OS saugumas yra tarsi sluoksniuotas pyragas:

1. Pačiame viršuje yra įrenginio gamintojo originalių programėlių parduotuvės saugumo sistema, kuri rūpinasi, kad kenkėjiškos programėlės nepatektų į parduotuvę. Paprastai programėlių parduotuvių savininkai atidžiai seka, kas pakliūva į jų parduotuvę.

2. Kitas sluoksnis – diegimo iš nežinomų šaltinių draudimas (angl. *Unknown Sources Warning*). Jis užtikrina, kad, kol jis veikia, niekas negali įdiegti jokių programėlių Jūsų įrenginyje iš nežinomų šaltinių, todėl tai yra paprastas ir labai efektyvus apsaugos būdas. Daugeliui vartotojų visiškai pakanka to, ką galima rasti įrenginio gamintojo programėlių parduotuvėje.

3. Už diegimo procedūros perspėjimų, kontrolės ir privilegijų patvirtinimo lygmenį yra atsakingas pats įrenginio naudotojas. Diegimo metu visos programos prašys leisti naudotis tam tikrais įrenginio ištekliais[3], kuriuos Jūs galite leisti arba uždrausti naudoti. Visada labai atidžiai peržiūrėkite, prie ko Jūsų diegiama programa nori gauti prieigą, kokiomis galimybėmis naudotis, kokias valdymo funkcijas perduodate programai, o jeigu Jums kyla abejonių, verčiau atsisakykite diegimo.

4. Toliau būtų trečiųjų šalių antivirusinės, saugios komunikacijos užtikrinimo ir kitos panašios programėlės, kurios įdiegtos Jūsų įrenginyje ir kontroliuoja turinį bei jame vykdomus veiksmus. Atkreipiame dėmesį, kad antivirusinė ir kita programinė įranga turėtų būti diegiama iš patikimų šaltinių.

Pasirūpinkite patys savo asmens duomenų saugumu

Taigi, Jūs įsigijote įrenginį su „Android“ OS. Nuo ko pradėti?

1. Pradėkite nuo užrakinimo. Būtinai naudokite užrakinimo funkciją, o įrenginiui atrakinti pasirinkite sudėtingą slaptažodį.
2. Slaptažodžiai ir PIN kodai. Nesaugokite jokių PIN kodų ir slaptažodžių atviru, nešifruotu tekstu, pvz., įrenginio užrašinėje. Naudokite tam specializuotas programėles (pvz., „KeePassDroid“), skirtas valdyti ir apsaugoti Jūsų slaptažodžius ir PIN kodus.
3. Vartotojų profiliai. Sukurkite keletą skirtingų vartotojų profilių įrenginyje skirtingiems žmonėms, pvz., vaikams, svečiams ir t. t. Tokiu būdu apsaugosite savo asmens duomenis nuo netyčinio ar tyčinio sunaikinimo ar perėmimo. Tai galite atlikti įrenginio meniu punkte „Nustatymai > Vartotojai“ (angl. *Settings > Users*).
4. Antivirusinė programa. Nesibaigianti virusų ir antivirusų kova vyksta ir šią akimirką, todėl būtinai, net jeigu nelabai kreipsite dėmesį į kitas rekomendacijas, naudokite gerą, patikimą

[1] Pažeistas įrenginio saugumas (angl. *compromised*) – bet kokia kenkėjiška programine įranga apkrėstas bet koks kompiuterinis įrenginys.
[2] OS PĮ (operacinės sistemos programinė įranga) – kompleksas programų, kurios valdo Jūsų įrenginį.
[3] Įrenginio ištekliai – įrenginio atmintis, procesoriaus darbo laikas, galimybė naudotis skirtingomis interneto prieigomis, visos kitos įrenginio funkcijos ir įdiegtos galimybės.

apsaugą nuo virusų, ir tai yra ta kategorija programų, kurioms rekomenduojama nepagailėti pinigų ir nusipirkti gerą, mokamą programos versiją.

5. Naudokite nuotolinio išvalymo (angl. *RemoteWipe*) funkciją. Tai galimybė praradus įrenginį per nuotolį jį ištrinti. Tokių programėlių yra daug, tokią funkciją greičiausiai turės ir Jūsų antivirusinė programa.

Komunikacijų saugumas

Viskas, ką Jūs siunčiate belaidžiu ar mobiliuoju (judriuoju) tinklu, naudodamiesi „Bluetooth“ jungtimi, teoriškai gali būti perimta, todėl pasistenkite kuo labiau apsisaugoti:

1. Belaidžiam tinklui naudokite tik WPA2 saugumo lygį Jūsų namų tinklo valdymo įrenginyje (angl. *router*), ilgą ir sudėtingą slaptažodį (15–30 ir daugiau simbolių, tarp kurių būtų didžiosios ir mažosios raidės, specialieji simboliai[4], skaičiai). **Nenaudokite WEP ar WPA su paprastais slaptažodžiais, o ypač „atvirų“, neapsaugotų tinklų**.
2. Atjunkite namų tinklo valdymo įrenginio, kuris dalija belaidį internetą Jūsų aplinkoje, WPS funkciją. Tai yra milžiniška spraga Jūsų saugumo sistemoje.
3. Yra speciali programų rūšis, kurios šifruoja Jūsų ryšį ir užtikrina saugų bendravimą duomenų tinklais, tad jos įspės apie bandymus perimti Jūsų duomenų srautus. Pasirinkite sau tinkamiausią (pvz.: „Hideninja VPN“, „WifiProtector“, „SecDroid“) ir, svarbiausia, diekite jas tik iš patikimų šaltinių.
4. Išjunkite „Bluetooth“ funkciją, tuo metu, kai jos nenaudojate.

Grėsmės, apie kurias nepagalvojate

1. Keičiate telefoną, planšetinį kompiuterį, o ar tikrai viską, kas gali suteikti informacijos apie Jus, ištrynėte negrąžinamai? **Patikrinkite dar kartą.**
2. Kortelės[5], USB atmintinės, išoriniai diskai – jeigu norite būti tikri, kad juose esantys duomenys nebūtų pasiekiami piktadariams, patys sunaikinkite juos fiziškai, t. y. **sukarpykite, sudeginkite** ar **sudaužykite**. Netgi iš sugedusių ar tokių duomenų saugyklų, kuriomis negalite pasinaudoti patys, duomenų vagys gali rasti galimybę nuskaityti duomenis.
3. Atnaujinimai, kuriuos vykdote. Nesunku imituoti ir pasiūlyti Jums esant nesaugioje aplinkoje (pvz., viešbutyje) netikrą atnaujinimą kuriai nors iš „gerųjų“ programėlių. Tokios atakos metu Jūsų įrenginys praneš, kad yra naujas atnaujinimas, pvz., „Adobe Flash“. Natūralu, kad Jūs leisite atsinaujinti. Kelios minutės ir jūsų įrenginio saugumas pažeistas – Jūsų įrenginyje veikia programėlė, kuri daro tai, kam Jūs turbūt nepritartumėte. **Todėl vykdykite atnaujinimus tik ten, kur esate santykinai saugūs, t. y. namuose, darbe.**

Nesusimąstėte, bet kai kurie veiksmai yra VISIŠKAI TEISĖTI, nors tai jums ir nepatiktų

1. Profiliavimas. Esama kompanijų, kurių pavadinimų Jūs niekada negirdėjote, bet jos savo serveriuose[6] yra sukaupusios informaciją apie Jūsų įpročius, pomėgius, sukūrusios Jūsų psichologinį ir elgesio modelį. Jos žino, kiek metų Jūsų vaikui, ką jis mėgsta, netgi tai, kokius sausus dribsnius valgote rytais, kada atostogausite ir kur, žino netgi tai, kad Jums už trijų mėnesių gims mergaitė.

---

[4] Specialieji simboliai yra šie: !, @, #, $, %, ^, &, *, (, -,), _, +, =, \, |, {, [, },], ”, ;, :, ’, <, ,>, /, ?.
[5] Kortelės – atminties, SIM ir kt.
[6] Serveris – labai galingas kompiuteris, tūkstančius kartų galingesnis už Jūsų įrenginį.

Kaip? Visa ko raktas – Jūsų naudojimosi telefonu ir elektroniniu paštu informacija. Jie išduoda Jūsų socialiniam tinklui arba Jūsų naršyklei, kokią reklamą Jums pateikti, kad Jūs pirktumėte prekes, kurios jums reikalingos (bet aišku, nebūtinai už geriausią kainą), per šiuos „išdavikus“ kompanijos susieja Jūsų įrenginį su profiliu, kurį kažkas saugo milžiniškuose duomenų centruose.

Ką daryti? Venkite palikti savo asmens duomenis pardavėjams, o jeigu tai būtina, **susikurkite profilį, kuris bus skirtas tik apsipirkimams ir brukalui[7], su netikrais asmens duomenimis.**

2. Stebėjimas. Žinokite, kad kai kurios įrenginyje esančios programėlės Jus seka – nustato Jūsų buvimo vietą, kartais atsisiunčia Jūsų adresų knygelę, kalendorius, žymeklius ar paieškų istoriją, pirkinių istoriją. Nelabai gražus elgesys, bet **leidimą tai daryti, greičiausiai, suteikėte Jūs patys, kai diegėte šią programėlę.**

Baigiant, dar kartą norėtume paraginti Jus būti atsargius ir budrius, nes nusikaltėliai nepraleis progos pasinaudoti Jūsų klaidomis.

Parengė Valstybinės duomenų apsaugos inspekcijos
Informacijos ir technologijų skyriaus
Vyriausiasis specialistas Andrejus Savkinas
Inspekcijos adresas internete *www.ada.lt*

Naudota literatūra:
http://lifehacker.com/how-secure-is-android-really-1446328680 (žiūrėta 2015-09-09).

[7] Brukalas (angl. *spam*) – nepageidaujami elektroniniai laiškai arba trumposios žinutės.