**Vilniaus Gedimino technikos universitetas**

**Elektronikos fakultetas**

**Kompiuterių inžinerijos katedra**

**Kompiuterių tinklai ir jų saugumas**

**Referatas**

**„Android saugumas“**

Studentas: Andrius Burbulis

Dėstytojas: Eimantas Garšva

Vilnius 2014

# Turinys

[Įžanga 3](#_Toc406094847)

[Pavojai 3](#_Toc406094848)

[Apsisaugojimas 8](#_Toc406094849)

[Išvados 9](#_Toc406094850)

# Įžanga

Android yra atviro kodo operacinė sistema, daugiausia naudojama išmaniuosiuose telefonuose, nors ją galima įdiegti ir kituose mobiliuosiuose įrenginiuose, kaip kad planšetiniame kompiuteryje. 2005 m. „Google“ įsigijo pirminį operacinės sistemos kūrėją, „Android Inc.“. 2007 m. buvo įsteigtas „Open Handset“ aljansas, kurį vienija 84 techninės bei programinės įrangos gamintojų ir telekomunikacijų bendrovės, atsakingos už šios operacinės sistemos tobulinimą. Tai Linux operacinės sistemos ir įvairių daugiausia „Google“ sukurtų papildomų plėtinių kombinacija. Pagrindinė šios sistemos programavimo kalba yra Java, kurios sintaksė ir daugelis pagrindinių klasių nesiskiria nuo Oracle siūlomos platformos, tačiau grafinės sąsajos API kitokia. Kuriamos programos sąsaja dalinai aprašoma XML. Java kodą vykdanti sistema kitokia ir neturi bendrų dalių su nuo seniau žinoma ir dabar Oracle priklausančia Java virtualia mašina. Visgi Oracle mano jog pasiūlydamas Android Google pažeidė jo įvairius programinės įrangos patentus bei pačios programavimo kalbos sukūrimo autorines teises ir šiuo metu bylinėjasi. Android turi papildomas priemones pasiekti akselerometrą, girometrą, GPS ir kitas sistemas kurios dažnos išmaniuosiuose telefonuose. Google yra sukūrusi internetinę Android programų ir modulių rinką, kur galima rasti apie 1,3 milijono įvairios kainos ir kokybės programėlių. Daugelis rinkoje pateikiamų programų ir modulių yra arba nemokami, arba kainuoja tik keletą dolerių. Dauguma telefonų gamintojų Android papildo įvairiais savo sukurtais plėtiniais. Android programos vykdomos „smėliadėžėje“, izoliuotos viena nuo kitos ir nuo operacinės sistemos. Rinkoje pasitaikė keletas prastai besielgiančių programų kurias „Google“ pašalino iš Interneto svetainės ir nuotoliniu būdu deaktyvavo tuose įtaisuose, kur jos buvo jau įkeltos. Jau siūlomos ir Android antivirusinės programos. Už „Google Play“ parduotuvėje parduotas programėles Google uždirba sutartą dalį rinkoje parduotos programos kainos.

2011 m. Android buvo populiariausia operacinė sistema mobiliesiems įrenginiams, naudojama apie 190 mln. įvairiausių įrenginių.

# Pavojai

Android OS vartotojai dažnai susiduria su įvairiais pavojais. Plačiai paplitęs atakos būdas prieš išmaniuosius telefonus yra sms žinutės su nuorodomis į užkrėstą turinį. Vienas iš žinomų tokio tipo atakų Lietuvoje buvo lotyniškomis raidėmis rusų kalba parašyta sms žinutė su nuoroda, siūlanti pasižiūrėti nuorodą. Vartotojai paspaudę ant nuorodos atvėrė savotišką Pandoros skrynią. Šis mėginimas baigėsi tuo, kad iš vartotojo telefono visi turimi adresatai gavo nuo 5 iki 20 SMS žinučių, apkrėstų interneto virusu. Negana to, sąskaitas už žinutes turi dar ir apmokėti. „Pabandžiau atsidaryti internetą telefone, nieko nepamačiau. Padėjau telefoną ir užsiėmiau savo reikalais“, – pasakojo vienas virusu užsikrėtusių vartotojų. Tokiais atvejais vartotojai labai nustemba, kadangi jie patys tokio turinio žinučių nesiunčia, tai atlieka pats viruso veikiamas išmanusis telefonas vartotojui nematant. Atlikus tyrimą, buvo nustatytas SMS žinutėse perduodamos nuorodos serverio adresas ir pavyko jį neutralizuoti. Todėl vėlesnis nuorodos paspaudimas grėsmės vartotojams nebekelia ir apkrėtimas virusu sustabdytas.

Vienas iš naujausių atakos būdų siejamas su duomenų vagimu ir vartotojų šantažu. ESET ekspertai paskelbė, jog neseniai atrado naują, Android operacinę sistemą veikiantį virusą. Skirtingai nuo ankstesnių, į išmaniuosius įrenginius nukreiptų kenkėjų, Android Simplocker yra pirmasis virusas, kuris pasisavina ir užšifruoja vartotojo duomenis ir mainais už jų atkodavimą reikalauja sumokėti nemažą sumą pinigų. Pasak ESET atstovų, iš pradžių pradėjęs veikti virusas nuskaito atminties kortelę ir ieško dokumentų pagal populiarius formatus, tokius kaip .jpeg, .png, .pdf, .doc, .mp4 ir kitus. Tuomet pavogus mobiliojo įrenginio duomenis, jie yra šifruojami, o savininkui siunčiama žinutė, reikalaujanti sumokėti išpirką. Kaip teigiama grasinime, laiku nesumokėjus pinigų, duomenys bus prarasti. Be to, psichologiniam spaudimui sustiprinti, vartotojui siunčiamos nuotraukos, kurios be asmens žinios padaromos jo išmaniuoju įrenginiu.

Mobilūs mokėjimai – tai atsiskaitymas už pirkinius išmaniuoju telefonu. Šis naujas atsiskaitymo būdas dar nėra plačiai naudojamas, bet ateityje turėtų sulaukti didelio populiarumo. Galimybė atsiskaitinėti pridėjus išmanųjį telefoną prie specialaus įrenginio ir įvedus PIN kodą atrodo ypač patraukliai. Šia paslauga gali naudotis tie, kurių išmaniuosiuose telefonuose įdiegta artimo atstumo duomenų perdavimo technologija - NFC (near-field communication) technologija. Lietuvoje panašiu principu jau veikia mobiliųjų mokėjimų sistema „MokiPay“, kuri taip pat leidžia už pirkinius atsiskaityti išmaniuoju telefonu. Tiesa, prie jo reikia prisiklijuoti specialų lipduką su NFC lustu. Taigi, ateityje turbūt pamatysime ne vieną mėginimą pasisavinti pinigus ar mokėjimo kortelių duomenis iš mobiliųjų įrenginių.

Klastingiausios mobiliųjų įrenginių programos yra skirtos prieiti prie asmeninės banko sąskaitos. Šiais metais „SophosLabs“ aptiko kenkėjišką programą, kuri veikdama kompiuteryje su „Windows“ sistema, įkelia „Trojos“ virusą į mobiliųjų telefoną per USB jungtį. Šio viruso tikslas yra perėmus visas SMS žinutes identifikuoti autentifikavimo kodus. Tai padarę nusikaltėliai gali netrukdomai prieiti prie Jūsų elektroninio pašto ar elektroninės bankininkystės.

Programėlių skirtų Android OS kiekiui tik augant, programėlės su slaptomis ir labai pavojingomis funkcijomis, tokiomis, kaip šnipinėjimas, tampa vienu didžiausių pavojų vartotojams. Probleminės aplikacijos yra super populiarios – jų parsisiuntimų kiekis jau viršija dešimtis milijonų. Su keletu saugumo spragas išnaudojančių programų (tarp jų ir gebančios perimti tinklu perduodamus duomenis) tyrėjai sugebėjo perimti iš „Android“ įrenginių (su 4.0 ICS versija) duomenis, įveikdami probleminių programėlių apsaugos priemones, kurios, kaip deklaruojama, naudoja TLS ir SSL protokolus. Kaip žinia, SSL ir TLS vieni populiariausių kriptografinių protokolų, užtikrinančių naršymo internete saugumą. Patys protokolai ir juose naudojamos technologijos laikomos saugiomis, tačiau nepakankamai saugi sertifikavimo centrų infrastruktūra, taip pat puslapiuose esančios klaidos lemia duomenų nutekinimą. Dabar prisidėjo ir dar viena silpnoji vieta – mobiliems įrenginiams skirtose programėlėse prastai sukurtos apsaugos priemonės. Pasinaudojant šiomis spragomis galima surinkti duomenis apie bankų sąskaitas, prisijungimus ir slaptažodžius prie PayPal, American Express ir kitų mokėjimų sistemų. Tap pat galima perimti autorizuotus duomenis, kurie skirti prisijungimui prie Facebook, elektroninio pašto ir debesų talpyklų bei perimti asmeninį susirašinėjimą ir netgi pasinaudoti IP kameromis. Vienas iš tokių aplikacijų pavyzdžių yra antivirusinė, į kurios duomenų bazę pavyko įrašyti pačių kūrėjų sukurtą kenkėjišką programą, su debesų talpyklomis leidžianti dirbti programą, kurią „naudoja keli milijonai žmonių, tačiau ji leidžia nutekinti prisijungimo duomenis dėl netinkamo SSL kanalo“, taip pat populiari WEB 2.0 klasės programėlė, kurią naudoja milijonai ir kuria lengvai nutekinami Facebook bei Google autorizacijos duomenys. Tarp skylėtų „Android“ sprendimų minima ir „daugelyje platformų naudojama staigiųjų žinučių apsikeitimo programėlė, kurios vartotojų skaičius perkopė 50 mln.“. Ji leidžia sužinoti telefonų numerius iš adresų knygos.

Mobilusis „Trojos“ virusas „Svpeng“, „Kaspersky Lab“ specialistų aptiktas šių metų vasarą ir galintis vogti pinigus tiesiogiai iš „Android“ išmaniųjų telefonų vartotojų banko sąskaitų, tapo įmantresnis. Dabar jis gali išvilioti ir vartotojų elektroninės bankininkystės prisijungimo duomenis, taikydamas netikruosius tinklalapius. Naujas šio „Trojos“ viruso funkcionalumas pasireiškia tuo, kad virusas pakeičia atverstą teisėto bankinio priedo langą netikru. Atitinkamai visi elektroninės bankininkystės sistemos prisijungimo duomenys, kuriuos vartotojas įveda šiame padirbtame lange, keliauja tiesiai į piktavalių rankas. Patekęs į išmanųjį telefoną virusas „Svpeng“ imasi priemonių apsisaugoti, o tai pasunkina jo aptikimą ir pašalinimą iš sistemos. Tokiu pat būdu „Trojos“ virusas „Svpeng“ bando pavogti ir aukos banko kortelės duomenis: kai paleidžiamas priedas „Google Play“, vartotojas išmaniojo telefono ekrane mato langą, kuriame jam siūloma įvesti savo mokėjimo kortelės numerį ir slaptą kodą. Šis netikro tinklalapio taikymo metodas leidžia apgavikams gauti tiesioginę prieigą prie patiklių arba neatidžių vartotojų finansinių duomenų. Per tris viruso „Svpeng“ gyvavimo mėnesius „Kaspersky Lab“ aptiko 50 šios kenkėjiškos programos modifikacijų, o apsaugos produktas „Kaspersky Internet Security for Android“ per šį laiką užblokavo daugiau nei 900 šio viruso nustatymų. Įdomu, kad patekęs į išmanųjį telefoną šis virusas imasi priemonių apsisaugoti, o tai pasunkina jo aptikimą ir pašalinimą iš sistemos. Pavyzdžiui, „Svpeng“ naudoja anksčiau nežinotą silpnąją „Android“ platformos vietą, dėl kurios gali sulaikyti telefono nustatymų grąžinimą į gamyklinius parametrus ir taip neleidžia jo pašalinti. Vienintelis priešnuodis „Kaspersky Internet Security for Android“ gali pašalinti šią kenkėjišką programą iš išmaniojo telefono. „Mobilusis „Trojos“ virusas „Svpeng“ platinamas su SMS šlamštu, kuriame kenkėjai dažnai taiko socialinės inžinerijos metodus: žinomų paieškos sistemų pavadinimus, intriguojamus pasiūlymus, žinomus vardus. Visa tai neturi suklaidinti vartotojų“, – pataria Romanas Unučekas, „Kaspersky Lab“ antivirusų ekspertas

Savo pastebėjimus kompiuterinių sprendimų specialistas Simon Szydor išsamiai aprašė tinklaraštyje „Snacks for your Mind blog”. Anot jo, Android programėlės gali fotografuoti iš išmaniojo įrenginio vartotojui net nepastebint – be jokių garsų ar šviesos efektų. Nematoma bus ir pati programėlė, o vieninteliai ženklai, galintys išduoti tokius veiksmus, gali būti tik greitai senkanti baterija ir didelis įrenginio procesų aktyvumas.

S. Szydor teigia, jog Google Play – kimšte prikimšta panašių šnipinėjančių programėlių. Daugumos jų tikslas – nuotoliniu būdu susirinkti informaciją (nuotraukas, įrašus, privačius duomenis), o pačiom išlikti nepastebėtoms.

Grynai moksliniais tikslais S. Szydor užsidegė sukurti tokią pačią, visiškai nepastebimą programėlę, leidžiančią slapčia fotografuoti iš išmaniojo įrenginio. Jis įvertino, jog tam užtenka vieno vienintelio pikselio. Taigi, šis tampa nematomas tokios aukštos raiškos išmaniuosiuose telefonuose kaip, pavyzdžiui, Nexus 5, su kuriuo tyrėjas atliko bandymus. „Rezultatai buvo nuostabūs ir gąsdinantys vienu metu,” – dalijosi įspūdžiais S. Szydor. – „To vieno pikselio ant ekrano pastebėti praktiškai neįmanoma, net jei ir žinai, kur tiksliai žiūrėti. Be to, net ir visiškai išjungus ekraną pikselio buvimas leidžia fotografuoti toliau.” Tokia šnipinėjanti programėlė gali slapta siųsti ne tik nuotraukas, bet ir kitą informaciją, pavyzdžiui, išmaniojo įrenginio buvimą vietą. Tam, kad pradėtų veikti, panašios programėlės turėtų būti instaliuojamos – tačiau S. Szydor tame problemos nemato. „Google Play prikimšta programėlių, kurios slapčia įdiegia ir papildomas aplikacijas, žinoma, vartotojo neatsiklausus,” – teigė jis. Jo žodžius patvirtina ir vienas autoritetingiausių verslo leidinių pasaulyje Forbes. Kaip teigia naujienų portalas Neowin, Forbes pranešime nurodoma, jog kai kurių programėles siūlančių tinklalapių „užkrėstumas” siekia net iki 33 procentų.

Suklastoti arba užgrobti belaidžiai tinklai yra vienas iš pažeidžiamumo būdų. Nemokamus belaidžius tinklus galima aptikti įvairiose vietose: kavinėse, restoranuose, parkuose, oro uostuose ir t.t. Augant nemokamų viešųjų belaidžių tinklų populiarumui, daugėja ir piktavalių, kurie klastoja arba užgrobia šiuos tinklus, siekdami šnipinėti vartotojus, pasisavinti jų prisijungimo vardus, slaptažodžius ar nukreipti juos į tinklalapius, platinančius kenkėjišką programinę įrangą.

Mobilieji „botnet“ tinklai tampa vis didesne grėsme. Šiandien daugelis išmaniųjų įrenginių yra prijungti prie interneto nuolatiniu 3G ar panašiu ryšiu. Mobilieji įrenginiai yra pakankamai galingi ir skaičiavimo pajėgumais prilygsta galingiems kompiuteriams. Saugumo ekspertai yra aptikę mobiliųjų „botnet“ tinklų formavimo pavyzdžių: „DROIDDREAM“ ar „GEIMINI“. „DroidDream“ naudojosi dviem „Android“ spragomis. Įvairių šaltinių duomenimis, 2011 metais buvo aptikta ne mažiau, nei 10 skirtingų mobiliųjų „botnet“ tinklų.

Kita „Android“ problema – programėlės, kurios, nors ir nėra kenkėjiškos, tačiau sukuria grėsmę asmens privatumui, saugumui bei prietaiso funkcionavimui. Tai – vadinamosios galimai nepageidaujamos programos (angl. potentially unwanted apps – PUA), kuriose agresyviai naudojama reklama, fiksuojama vartotojo buvimo vieta, jo kontaktinė informacija. Kai kurios PUA programėlės yra skirtos vartotojui apgauti ir priversti mokėti už paslaugas, kurių vartotojui nereikia. Pavyzdžiui, trečiųjų šalių „Android“ programėlių parduotuvėse „SophosLabs“ neseniai aptiko žaidimą, kuris mėgdžioja populiarų „Flappy Bird“. Realybėje, ši programėlė skirta apgauti vartotoją – ji siunčia SMS žinutes į padidinto tarifo numerius, o mokestis už jas nuskaitomos iš vartotojo sąskaitos.

Facebook sprendimas išleisti dar vieną programėlę, skirtą atskirai tik žinučių siuntimui, sukėlė nemažą vartotojų nepasitenkinimą. Atrodo, be pačios Facebook vadovybės, mažai kas supranta, kam to reikia. Tačiau per šį savaitgalį nepasitenkinimas peraugo į pasipiktinimą. Milijonams vartotojų jungiantis prie naujosios Messenger aplikacijos, aiškėja, kokias galimybes turi įdiegta programėlė. Sudėjus jas kartu laisvai galima pamanyti, jog kišenėje nešiojiesi šnipinėjančią programą. Kaip teigia solidus JAV naujienų laikraštis „The Washington Post”, Facebook palaipsniui verčia savo vartotojus prisijungti prie Messenger‘io. Nepalikus galimybės dalyvauti pokalbiuose įprastoje Facebook aplikacijoje, vartotojai nori nenori turi įsidiegti specialią žinučių siuntimo programėlę. Facebook atstovė spaudai į kaltinančius klausimus atsakė, jog jų tikslas yra sukurti pačią geriausią susirašinėjimo programėlę ir išvengti nepatogumų, kuriuos gali patirti vartotojai. Vis dėlto apie konkrečius nepatogumus užsiminta nebuvo. Tuo tarpu didžiausi pasaulio dienraščiai ir portalai analizuoja Messenger‘io galimybes ir stebisi, kas norėtų tokią programėlę įsidiegti. Kaip taikliai pastebi „Cosmopolitan”, Facebook Messenger iš esmės gali kontroliuoti visą išmanųjį įrenginį. Štai ko reikalauja programėlė, jeigu norite ją įsidiegti:

* keisti prisijungimo prie interneto būseną (gali išjungti ar įjungti įrenginio Wi-fi);
* savarankiškai skambinti ir siųsti SMS žinutes;
* bet kuriuo metu įrašinėti garsą, vaizdą ir fotografuoti;
* peržiūrėti skambinimo istoriją ir kalendoriaus įvykius;
* analizuoti bendravimo su kitais žmonėmis dažnumą ir pobūdį;
* skaityti asmeninės vartotojo paskyros informaciją;
* turėti priėjimą prie įrenginio ID ir telefono numerio;
* Gauti įdiegtų įrenginyje programėlių kitų vartotojo paskyrų sąrašą.

Taigi, parsisiuntus Facebook Messenger, teoriškai šiai programėlei suteikiama galimybė stebėti viską, ką vartotojai veikia. Įtariame, jog kiekvienas pažįstate bent vieną žmogų, kuris visą savo gyvenimą stengiasi sutalpinti į mažytį Facebook‘o ar Twitter‘io puslapėlį. Dėl ko – pripažinimo, įvertinimo ar „šiaip”, geriausiai žino tik jie patys. Tačiau pasirodo kartais net nereikia stengtis, kad tavo gyvenimas būtų sekamas, o nuotraukos peržiūrimos. IT specialistas S. Szydor atrado, jog spraga Android operacinėje sistemoje leidžia nematomoms programėlėms slapčia fotografuoti ir siųsti šias nuotraukas per visą internetą.

Pavogti ar pamesti išmanieji įrenginiai yra rimta grėsmė. Išmaniuosiuose telefonuose ir planšetiniuose kompiuteriuose saugoma labai daug vertingų duomenų. Nemalonu prarasti asmeninius duomenis, o praradus kompanijos duomenis gali kilti ir rimtų problemų. Ši problema aktualesnė mažoms įmonėms, kurios neturi lėšų saugumui mobiliuosiuose įrenginiuose užtikrinti. Šių įmonių darbuotojai dažniausiai naudojasi tuo pačiu įrenginiu darbe ir namuose, todėl tai gali sukelti papildomų grėsmių.

Išmaniųjų telefonų ir planšetinių kompiuterių savininkai neturėtų pasikliauti standartine trynimo funkcija. Naujausi atlikti tyrimai rodo, jog rankiniu būdu ištrinti duomenis gali būti lengvai atkuriami. Įrenginiuose esanti funkcija „Reset” duomenų nesunaikina, todėl perleisdami savo telefoną, savininkai rizikuoja visa jame buvusia informacija. Pateikiamoje ataskaitoje aprašomi du tyrimai – vienas skirtas Android išmaniesiems telefonams, kitas planšetiniams kompiuteriams. Eksperimente panaudoti įrenginiai buvo gauti iš „antrų rankų” turgaus – vietos, kurioje galima įsigyti naudotų daiktų. Tyrimo metu buvo siekiama nustatyti, kiek tariamai ištrintos informacijos įmanoma atkurti. Paaiškėjo, jog net ir pasinaudojus kiekviename įrenginyje esančia „Reset” (liet. iš naujo nustatyti) funkcija, vidinėje atmintyje esantys duomenys apskritai nėra ištrinami. Vietoje to tik pašalinamos į šią informaciją nukreipiančios nuorodos. Taigi, pasinaudojus santykinai paprastais programiniais įrankiais, kaip ir padarė tyrėjai, visą įrenginyje buvusią informaciją galima atkurti lyg ji niekada nebūtų trinta. Pasaulinė duomenų trynimo sprendimų lyderė „Blancco” ne kartą yra pabrėžusi sertifikuotų produktų svarbą. Ir šį kartą, pasiteiravus jos nuomonės apie tyrimo rezultatus, „Blancco” teigia, jog nėra nustebinta. „Tai, kad gamybinė duomenų naikinimo funkcija nėra veiksminga, mums jau seniai žinoma”, – sako Kim Väisänen, „Blancco” valdybos direktorius. – „Negrįžtamai duomenis sunaikina tik specialiai tam skirti produktai, tokie kaip, pavyzdžiui, „Blancco Mobile”.K. Väisänen pabrėžia, jog tiek pavieniai vartotojai, tiek įmonės turėtų būti atsargūs perparduodami ar atiduodami nebereikalingus išmaniuosius įrenginius. Be to, jie turėtų įsitikinti, kad jų ryšio operatoriai ar įrenginių pardavėjai naudoja atitinkamus duomenų trynimo produktus. Tik taip įmanoma užtikrinti perparduodamų įrenginių saugumą. „Tikrasis duomenų trynimas vykdomas operacinės sistemoje lygmenyje”, – aiškina „Blancco” valdybos direktorius. – „Sertifikuoti ir patikrinti programiniai sprendimai taikomi ne dėl to, kad jais greičiau ar patogiau ištrinama informacija. Tiesiog jie tai atlieka iš tiesų – sunaikina duomenis negrįžtamai”.

# Apsisaugojimas

Slaptažodis: visi girdėjo, retas vartoja. Reikalavimas užrakinti telefoną slaptažodžiu visiems pažįstamas „iki skausmo“ ir girdėtas ne kartą. Tačiau, anot T. Jokubausko, į jį daugelis vartotojų, net savo išmaniuosiuose įrenginiuose kaupiantys slaptą verslo informaciją, dažnai numoja ranka. Saugumo specialistai pataria – turėti bent 4 skaičių PIN kodą išmaniajame telefone yra būtina. Taip pat galima pasirinkti specialų prabraukimo modelį (angl. „swipe pattern“). Tiesa, tokį slaptažodį, kitam asmeniui perėmus išmanųjį įrenginį, gali išduoti nešvarių pirštų ant ekrano paliktos žymės. Saugiausias variantas apsaugoti išmanųjį telefoną – pasirinkti stiprųjį slaptažodį, kurį sudaro didžiųjų ir mažųjų raidžių, skaičių, simbolių ir tarpelių kombinacija.

Nustatykite automatinį įrenginio užrakinimą. Jeigu apsaugojote savo išmanųjį telefoną slaptažodžiu, bet palikote jį ant stalo neužrakintą, tarkime, 15 minučių, pasiekti telefone esančius duomenis nebus labai sunku. Daugelis išmaniųjų telefonų turi automatinio užrakinimo funkciją, tad, jeigu ji dar nenustatyta, įjunkite ją. Pasak saugumo specialistų, geriausia pasirinkti kuo trumpesnį užsirakinimo periodą: 2-5 minutės yra geriau nei 10-30 min. Nuolat užsirakinantis telefonas gali sukelti nepatogumų, tačiau tai menkniekis palyginti su prarastais svarbiais duomenimis ar kontaktais.

Rinkitės patikimą išmaniųjų programėlių šaltinį. Prieš susiviliodami diegti vieną ar kitą programėlę, visų pirma atidžiai rinkitės šaltinį, iš kurios ją ketinate parsisiųsti. Tarkime, tokie puslapiai kaip „Google Play“ ir „Apple Store“ taiko griežtus saugumo standartus, atidžiai renkasi, kokios programėlės gali būti pasiekiamos vartotojui. Nepaisant to, prieš diegdami bet kokią programėlę net ir iš patikimo šaltinio, atidžiai perskaitykite prieš tai ją parsisiuntusių vartotojų atsiliepimus ir vertinimus, patikrinkite, ar daug žmonių ją jau išbandė.

Neleiskite programėlei peržengti ribų. Diegdami programėles į savo išmanųjį telefoną ar kitą įrenginį, atkreipkite dėmesį, kokias teises joms suteikiate: ar leidžiate pasiekti savo kontaktus, nuotraukas, fiksuoti buvimo vietą ir pan. „Synergy Consulting“ vadovas T. Jokubauskas, vertinant programėlės prieigos ribas, pataria pasitelkti logiką. Pavyzdžiui, tikėtina, kad SMS programėlė paprašys leidimo siųsti ir gauti žinutes, žemėlapio programėlė – leidimo nustatyti jūsų buvimo vietą pasitelkus GPS, o susirašinėjimui ar interneto pokalbiams skirta programėlė norės prisijungti prie kontaktų, nuotraukų, vaizdo ir garso įrašų. Pavyzdžiui, „Facebook“ susirašinėjimo programėlė prašo prieigos prie nuotraukų tam, kad vėliau vartotojas galėtų jomis dalintis su savo draugais. Tačiau verta sunerimti, kai nuotraukų apdorojimo programėlė prašo prieigos prie telefone esančių kontaktų arba lažyboms skirta programėlė – prieigos prie el. bankininkystės sistemos.

Nepamirškite atnaujinti išmaniojo įrenginio programinės įrangos. Neretai naujai rinkai pristatomų produktų programinėje įrangoje būna įvairių saugumo spragų. Tačiau gamintojai suinteresuoti savo programinės įrangos kokybės gerinimu, todėl nuolat diegia jų atnaujinimus, kurie padeda užskirsti kelią įsilaužėliams į išmaniuosius įrenginius.

Nespauskite ant kiekvienos nuorodos el. laiške ar žinutėje. Išmaniajame telefone, kaip ir kompiuteryje, paspaudus ant „kenkėjiškos“ nuorodos galima įdiegti kenksmingus atnaujinimus. Nereiktų pamiršti, kad išmaniuosiuose įrenginiuose pavojingos nuorodos plinta ir žinutėmis. Dažnai tokios nuorodos vilioja patraukliu el. laiško pavadinimu ar galimybe ką nors gauti nemokamai, o kartu prašo asmeninių duomenų. Anot T. Jokubausko, net nespausdami ant nuorodos, o tik atsakydami į nežinomo siuntėjo el. laišką ar žinutę išmaniajame įrenginyje, vartotojai gali pritraukti nesąžiningų asmenų ar grupuočių dėmesį, kurie gali pradėti intensyvesnes atakas.

Užšifruokite savo išmanųjį įrenginį (angl. „encryption“). Tokia priemonė rekomenduojama, jei telefone saugoma labai svarbi informacija. Nepamirškite, kad net ir slaptažodžiu apsaugotą telefoną, vagystės atveju nesąžiningas asmuo gali lengvai prijungti prie kompiuterio bei taip gauti prieigą prie jūsų asmeninių duomenų.

Išjunkite WiFi ir „Bluetooth“ prieigas, kai jomis nesinaudojate. Tuo metu, kai nenaudojate WiFi arba „Bluetooth“, geriausia, kad šios programėlės būtų išjungtos. Tereikia išmaniojo įrenginio nustatymuose pasirinkti tokią funkciją. Taip pat kiekviename įrenginyje galima nustatyti, kad jis automatiškai prisijungtų tik prie gerai pažįstamo – namų ar darbo – tinklo, o „Blootooth“ ryšys būtų įjungiamas tik suteikus leidimą. Kitu atveju išmanusis įrenginys gali automatiškai prisijungti prie tinklų ar įrenginių, kurie yra nepatikimi, gali perimti duomenis apie jūsų buvimo vietą ir pan. Prisijungus prie viešo WiFi tinklo, patartina nesinaudoti aplikacijomis, kurios apdoroja svarbią informaciją, nes taip yra rizika nukentėti nuo MIM atakos. „Man-in-the-middle“ ataka (dažnai sutrumpintai vadinama MITM, MitM, MIM, MiM, MITMA, taip pat žinoma kaip „bucket brigade“ arba „Janus“ ataka) yra aktyvi slapto pasiklausymo forma, kai, pasitelkęs nesaugų Wifi ryšį, užpuolikas gali įterpti save tarp dviejų pašnekovų. Iš čia kilęs ir atakos pavadinimas „žmogus viduryje“ (angl. „Man-in-the-middle“).

Įdiekite išmaniajame įrenginyje saugos programinę įrangą (angl. „security software“). Išmanieji telefonai yra kompiuteriniai įrenginiai, tad ir jiems apsaugoti kuriama atitinkama programinė įranga. Tam diegiamos specialios programėlės, kurios pasirūpina kenkėjiškų programų prevencija, nuotoliniu būdu ištrina nereikalingus duomenis, peržiūri kitų programėlių privatumo nustatymus ir reikalavimus, siunčia automatinius perspėjimus keičiant prietaiso nustatymus.

# Išvados

Naudodami mobiliuosius įrenginius su pavojais susiduriame kiekvieną dieną. Populiarėjant mobiliesiems mokėjimams, m. parašo paslaugai, išmaniųjų namų sprendimams bei naudojant įrenginius su „Android“ OS darbe, ypač didelėse įmonėse, keliame vis didesnį įsilaužėlių susidomėjimą. Statistika rodo, kad virtualiai pavogiamų pinigų sumos yra vis didesnės ir galima drąsiai teigti, kad jos nuolat didės. Tai įrodo, kad į mobiliųjų įrenginių saugumą privaloma žiūrėti rimtai ir imtis visų įmanomų saugumo priemonių bei pagalvoti prieš diegiant naują aplikaciją, atsidarant neįprastą nuorodą ar bylą, vengti bankinių pavedimų ir nesinaudoti internetu, kai tai nėra būtina. Atsakingai naudojantis išmaniaisiais įrenginiais pajusime jų teikiamą naudą ir išvengsime įsilaužėlių daromos žalos bei nemalonumų.