

Standartinė iOS telefono apsauga

Deividas Ambrazevičius

Aug 18, 2025

Įžanga

Šiandien telefonas tai tavo gyvenimo juodraštis, jame tavo tapatybė, šeimos nuotraukos, darbinių pokalbių fragmentai, banko ir socialinių paskyrų raktai, maršrutai iki namų ir vietos, kuriose lankaisi. Jei kas nors perima telefoną arba jo duomenų srautus, jis gauna daugiau apie tave, nei papasakotum artimam draugui. Gera žinia tokia, kad vien tik standartiniais iOS įrankiais gali stipriai sumažinti riziką. Ir tai nėra paranoja, tai higiena, kaip dantų valymas.

Kokios yra realios grėsmės?

Socialinė inžinerija ir „phishing“ - gudriai pateikta SMS/žinutė su „VMI“ priedu ar „paskyros atnaujinimu“ prašo suvesti slaptažodį ar įdiegti profilį. Vienas paspaudimas ir atiduodi prisijungimus arba net savo turtą..

Paskyros perėmimas be telefono vagystės - užtenka SIM perrašymo (SIM-swap), slaptažodžio pakartotinio naudojimo ar užgrobtos el. pašto dėžutės. Tu dar turi telefoną, bet kažkas jau keičia slaptažodžius tavo vardu.

Lokacijos sekimas ir metaduomenys - net jei nesi „įsilaužėlių“ taikiny, reklamos identifikatoriai, be reikalo įjungta „Wi-Fi/Bluetooth“, „Location Services“ ir programėlių leidimai paverčia tave judančiu švyturiu. Iš maršrutų galima atsekti namus, darbą, vaiko mokyklą.

Nereikalingi sistemos „kraneliai“ - diagnostika, „Suggestions“, foniniai atnaujinimai, automatiniai atsisiuntimai, visa tai kuria ne tik triukšmą ir eikvoja bateriją, bet ir padidina atakos paviršių.

Debesų (iCloud) patogumo kaina - automatinis sinchronizavimas be E2EE arba silpna 2FA reiškia, kad nutekėjus Apple ID - nuteka viskas: nuotraukos, kontaktai, užrašai, atsarginės kopijos.

Trumpai tai nereikia "nulaūžimo", dažniausiai užtenka įtikinti spustelėti arba palikti įjungtus dalykus, kurių tau nereikia.

Kodėl verta tai daryti?

Informacijos rinkimas apie jus. Numatyti "iOS" nustatymai leidžia daugeliui paslaugų rinkti diagnostiką, naudojimo statistiką, vietos duomenis. Išjungus tai, sumažėja jūsų skaitmeninis šešėlis.

Atakos paviršius. Kuo mažiau leidimų turi programėlės (kamera, lokacija, foninis atnaujinimas), tuo sunkiau piktavaliams pasinaudoti klaidomis ar socialine inžinerija.

Kontrolė ir švaresnė patirtis. Slopindami triukšmą (pranešimus, siūlymus, automatinius atnaujinimus) patys sprendžiate, kada ir ką daryti, o ne atvirkščiai.

Teisinė bei fizinė rizika. Biometrika patogė, bet tam tikrose situacijose (priverstinis atrakinimas) saugesnis yra **PIN**. Padėsime susiderinti balansą.

Dėmesio: šie žingsniai nepaverčia telefono neįsilaužiamu, tačiau ženkliai sumažina rizikas be jokių papildomų įrankių, norint jį paversti neįsilaužiamu, reikėtų pirkti atskirą telefoną bei perdaryti visą jo vidinę sistemą nuo pat pradžių, jei domina - Kreipkis: (Signal: davidamber.28)

Esminiai privatumo ir saugumo nustatymai

Pranešimai ir ryšiai "patogumai" dažnai yra silpnos vietos socialinei inžinerijai ir duomenų nuotėkiui.

Rekomendacijos skirtos "saugesniam pagal nutylėjimą" naudojimui; *kai kuriuos dalykus prireikus įsijungsite laikinai.*

1) Pranešimai, ryšiai, „triukšmo“ mažinimas

- **Settings > Notifications**
 - **Show previews: Never/When unlocked** - pranešimų turinys nerodomas užrakintame ekrane, saugoma privati informacija.
 - **Screen Sharing: Off** - pranešimai nerodomi dalijantis ekranu, apsauga nuo informacijos nutekėjimo.

- **Siri Suggestions: Disable all** - Siri nebesiūlys veiksmų pagal tavo naudojimą.
- **Disable notifications on sensitive apps** - jautrių programų (pvz., banko, slaptažodžių) pranešimai išjungiami.
- **Settings > General**
 - **AirDrop > Receiving Off** - niekas negali siųsti failų per AirDrop.
 - **AirDrop > Bringing Devices Together: Disabled** - automatinis persijungimas pagal įrenginių artumą išjungtas.
 - **AirDrop > Use Cellular Data: Disabled** - AirDrop nenaudoja mob. duomenų.
 - **AirPlay & Handoff: Disable all** - išjungiamas automatinis turinio perdavimas tarp įrenginių
 - **Picture in Picture: Disabled** - vaizdo langai nefiksuojami ekrano kampe.
 - **iPhone Storage > Recently Deleted Album: Enable** - išsaugomas "Neseniai ištrintų" albumas.
 - **Standby: Disabled** - telefonas neišjungia ekrano į "standby" režimą..
- **Settings > Bluetooth: Off** (jei nenaudojate) - Bluetooth yra visiškai neapsaugotas kanalas, lengvai prieinamas, skleidžia identifikatorius, o išjungus juos nebesiseka to daryti, idealiausiu atveju įsijungti jį tik tada, kai naudojate.

Vietos nustatymas

Vietos duomenys yra viena jautriausių kategorijų. Laikinas įjungimas tik kai reikia užkerta kelią istorijų kaupimui.

- **Settings > Privacy & Security > Location Services: Disable all.**
- Kai prireikia žemėlapių ar maršrutų, trumpam įjunkite ir griežtai apkarpykite leidimus:
 - Programėlėms - **"Never"** arba **"While Using the App"**, be **Precise Location**.
 - **Settings > Privacy & Security > Location Services > System Services:**
 - Apple Pay, Find My iPhone*, HomeKit, Share My Location, Suggestions & Search, System Customization, Significant Locations, iPhone Analytics, Improve Maps – **Disabled**.
 - Baigę – vėl grįžkite prie **Location Services: Disabled**.

* - įsitikinkite, kad nepamesite telefono:)

Sekimas, analizė ir reklama

Tai sisteminiai duomenų "kraneliai", juos užsukus, jūsų aktyvumas nekeliauja į analitikos sistemas.

- **Settings > Privacy & Security > Tracking: Disable all** - jokių programėlių sekimo leidimų.
- **Settings > Privacy & Security > Analytics & Improvements: Disable all** - nebesiunčiame diagnostikos į Apple serverius.
- **Settings > Privacy & Security > Advertising > Personalized Ads: Disabled** - mažiau profiliavimo, tai reiškia, kad dažnai nebematysite reklamų kas liečia jūsų naršymo istoriją ar pokalbius.
- **Settings > Privacy & Security > Research Sensor & Usage Data: Disable all** - išjungiame įrenginio naudojimo ir jutiklių duomenų siuntimą tyrimams ar "Apple" tobulinimui.
- **Settings > Privacy & Security > Motion & Fitness: Disable all** - sustabdomas judesio, žingsnių, treniruočių bei fizinės veiklos stebėjimas per įrenginio jutiklius.
- **Settings > Privacy & Security > Journaling Suggestions: Disable all** - išjungiamos automatinės dienoraščio (Journaling) programos siūlomos mintys ar priminimai, paremti naudojimo duomenimis.
- **Settings > Privacy & Security > Sensitive Content Warning: Disabled** - nebus automatiškai perspėjama dėl jautraus turinio (pvz., galimai šokiruojančių ar nepageidaujamų nuotraukų/žinučių).

„Safari“ ir naršymas

Naršyklė didžiausias sekimo kanalas. Mažiname identifikavimo galimybes ir paliekame mažiau pėdsakų.

- **Settings > Safari**
 - **Prevent Cross-Site Tracking: Enabled** (apsauga nuo sekimo tarp svetainių).
 - **Fraudulent Website Warning: Disabled** – šis patarimas mažina užklausas į trečiųjų šalių tikrinimo sąrašus; **trade-off**: negausite "phishing" įspėjimų. Jei dažnai spaudžiate nuorodas iš SMS/El. pašto - palikite **Enabled**.
 - **Search Engine: DuckDuckGo** (mažiau profiliavimo).

- **Siri & Search: Disable All, Search Engine Suggestions: Disabled, Safari Suggestions: Disabled.**
- **Quick Website Search: Disabled, Preload Top Hit: Disabled.**
- **AutoFill: Disable All** - kreditinių kortelių ir adresų autofill'as yra patogus, bet jautrus.
- Kartą per savaitę(jei norima): **Settings > Safari > Clear History and Website Data > All history** ir **Close All Tabs**.

Žinutės ir skambučiai

Jei jums nebūtina "iMessage/FaceTime", jų išjungimas sumažina atakos paviršių ir duomenų srautą. (Jei naudojate - palikite įjungtus, bet ribokite pranešimus ir bendrinimą.)

- **Settings > Messages**
 - **iMessage: Disabled, Share Name and Photo: Disabled.**
 - **Shared with You: Disabled, Show Contact Photos: Disabled.**
 - **Notify Me: Disabled.**
- **Settings > FaceTime > FaceTime: Disabled.**

Foninis atnaujinimas (Background App Refresh)

Foniniai atnaujinimai reiškia nuolatinį tinklo aktyvumą ir lokacijos užklausas. Išjungus - baterija ir privatumas laimi.

Settings > General > Background App Refresh: Off

Ir papildomai - atskiruose įrašytuose Apple app'uose: **Apple Store, Music, Notes, Numbers, Pages, Shortcuts, Siri, Voice Memos – Disabled.**

Kamera ir nuotraukos

Mažiname automatinį turinio atpažinimą ir fono užklausas.

- **Settings > Apps > Camera > Scan QR Codes: Disabled** - išvengiama netyčinių atidarymų.
- **Settings > Apps > Photos > Enhanced Visual Search: Disabled.**

„App Store“ ir atnaujinimų strategija

Rankinė kontrolė reiškia, kad atnaujinimai nepasibels blogiausiu laiku (pvz., per mobilų ryšį) ir nesuveiks automatiniai perjungimai.

- **Settings > App Store**
 - **Video Autoplay: Off**
 - **In-App Ratings & Reviews: Disabled**
 - **Disable “App Downloads”, “App Updates”, and “In-App Content” (Automatic Downloads)** - viską atnaujinsite rankiniu būdu.
- Kartą per savaitę:
 - Atidarykite **App Store**, viršuje spauskite **profilio ikoną**, **pull-to-refresh**, spauskite **Update All**.
 - **Settings > General > Software Update** - patikrinkite ir įdiekite „iOS“ atnaujinimus (geriausia per Wi-Fi).

Mobiliojo ryšio „ugniasienė“

Paprastas, bet galingas būdas apriboti netyčinį foninį srautą naudojant mobilų ryšį.

- **Settings > Cellular** - išjunkite prieigą prie duomenų programėlėms, kurioms mobilus internetas nereikalingas (pvz., Find My, Contacts ir pan., jei nedera su jūsų scenarijumi).

Mikrofonas

Ar nutuokėte kiek programėlių turi prieigą prie jūsų mikrofono 24/7? Geras būdas užkirsti tam kelią.

- **Settings > Privacy & Security -> Microphone** - Išjungiamo programų prieigą prie mikrofono, kad jos negalėtų mūsų klausytis ar įrašinėti garso be leidimo.

Slaptažodžiai ir automatinis pildymas

Jei slaptažodžius laikote kitur, išjungtas „Autofill“ – mažiau atakos vektorių.

- **Settings > Passwords > Password Options > Autofill Passwords: Disabled.**
- **Settings > Battery > Battery Percentage: Enabled** (ne apie privatumą, bet padeda planuoti:)).

Biometrija: Touch ID vs Face ID

- Pirštas (**Touch ID**) paprastai saugus ir **nekeliauja** į „Apple“ - tai matematinių šablonų palyginimas įrenginyje.
- **Face ID** taip pat lokaliai apdoroja duomenis, bet kai kuriems žmonėms rizikingesnis fizinio spaudimo scenarijuose.

Prievartinė prieiga, teisėsaugai kai kuriose šalyse gali būti lengviau jūsų paprašyti piršto ar veido nei PIN. Dėl to **stiprus PIN** - būtinas, o jei neramu, naudokite tik PIN ir **išjunkite biometriką**.

„iCloud“ ir atsarginės kopijos

Vietinė šifruota kopija sumažina priklausomybę nuo debesies ir geriau valdo, kas turi prieigą prie jūsų archyvų.

- Jeigu įmanoma - nenaudokite iCloud jautriems dalykams.
- Jei būtinai reikia, darykite taip:
 - **Settings > [TAVO VARDAS] > iCloud - Advanced Data Protection for iCloud: Enabled** (end-to-end šifravimas daugumai duomenų).
 - Įjunkite **stiprią 2FA**
- **Vietinės, užšifruotos kopijos (rekomenduojama):**
 - Mac'e atidarykite **Finder**, prijunkite „iPhone“ per USB.
 - Kairėje pasirinkite įrenginį, pažymėkite **„Encrypt local backup“**, susikurkite slaptažodį, spauskite **„Back Up Now“**.

- Nuotraukoms vietoje "Photos/iCloud Photos" naudokite minimalistinę Image Capture(ar betkokią kitą) programą, prijunkite telefoną, pasirinkite paskirties folderį, **Import All**, o prireikus - ištrinkite turinį iš telefono.

Papildomi, bet naudingi patobulinimai

Kuo mažiau sisteminių "kabliukų", tuo mažiau foninio srauto bei rinkimo.

- **Settings > Apps > Safari > Advanced > Privacy Preserving Ad...: Disabled** ir **Check for Apple Pay: Disabled** - sumažina fonines integracijas.
- **Settings > Apps > Maps - Share ETA, Air Quality Index, Weather Conditions, Ratings & Photos, Show Ratings and Photos Suggestion, Follow Up by Email - Disabled.**
- **Settings > Apps > Shortcuts - iCloud Sync: Disabled, Private Sharing: Disabled.**
- **Remove stock apps** (Home, Translate, Books, etc.) - ilgai paspauskite ikoną > **Remove App > Delete App.**

Pabaigai

Šis gidas aprašo tik standartinius "iOS" viduje pasiekiamus nustatymus, tai bazinė higiena, ženkliai mažinanti rizikas be jokių papildomų įrankių. Tačiau jei jūsų tikslas yra maksimalus privatumas ar net veikimas anonimiškai, tam prireiks atskiros, specialiai paruošto įrenginio ir griežtesnio "hardening", alternatyvių konfigūracijų be ekosistemos priklausomybių, atskirų SIM/eSIM strategijų, atskirtų paskyrų bei griežtos ryšio higienos. Galiu padėti tai įgyvendinti, nuo poreikių ir grėsmių modelio įvertinimo iki telefono parinkimo, paruošimo "nuo nulio" ir kasdienio naudojimo gairių (atskiri profiliai darbui/kelionėms, vienkartinės paskyros, saugių kanalų pasirinkimas).

Ryšio kontrolei egzistuoja ir specialūs sprendimai, pasyvūs (pvz., ekranavimo/"Faraday" dėklai), programiniai "no-radio" profiliai bei įrangos jungikliai, leidžiantys fiziškai ar programiškai apriboti įrenginio skleidžiamus signalus. **Atkreipiu dėmesį**, kad aktyvūs radijo ryšio slopintuvai ("jammers") daugelyje šalių yra draudžiami, naudokite tik teisėtus metodus ir laikykitės galiojančių įstatymų.

Jei norite eiti toliau nei standartiniai nustatymai, parašykite, paruošiu konkretų planą, pakonsultuosiu, sukomplektuosiu įrankius ir įrenginį pagal jūsų grėsmių modelį bei poreikius.
(Signal: **dauidamber.28**)

Powered by D. Ambrazevicius