Slaptažodžiai ir FIDO: Planas, kaip sustiprinti savo paskyras

Deividas Ambrazevičius Sep 20, 2025

Įžanga

Nuo namų durų iki mokyklos ūkvedžio raktų ryšulio, esame įpratę prie minties, kad kiekvienai spynai reikia atskiro rakto. Tad nenuostabu, kad ir mūsų skaitmeniniame gyvenime atsirado begalės skirtingų raktų: slaptažodžių, PIN kodų, ir pan. Tačiau čia ir slypi didžiausias pavojus: įsivaizduokite, jei mokyklos ūkvedys naudotų vieną ir tą patį raktą serverinei, direktoriaus kabinetui ir slaptų dokumentų seifui - įsilaužėliams tai būtų lengviausia užduotis. Tad kodėl rizikuojate savo skaitmeniniu gyvenimu naudodami vieną slaptažodį visur? Taip pat atsiradusios biometrikų autorizacijos stipriai palengvina visiem gyvenimus.

Būtent dėl to paruošiau jums praktišką ir aiškų planą, kaip per vieną savaitgalį galite sustiprinti savo svarbiausių paskyrų apsaugą. Šis planas paremtas patikrinta patirtimi ir geriausiomis praktikomis.

Padėkite sau, draugams, savo šeimos nariams bei savo draugų šeimos nariams apsisaugoti ir bent supažindinti su biometriką šiuolaikiniame pasaulyje.

Slaptažodžiai

Negalvok slaptažodžių pats, tegu generuoja slaptažodžių tvarkyklės, lai generuoja 24+ ilgio slaptažodžius į kuriuos įeitų didžiosios mažosios raidės, skaičiai ir specialūs simboliai. Atsimink tik porą dalykų**:** Kompiuterio slaptažodį/PIN ir slaptažodį, kuriuo atrakini slaptažodžių tvarkyklę.

Trumpai:

- Vienas slaptažodis = viena paskyra
- Naudokite automatinius generatorius slaptažodžiams generuoti
- Kurkite ilgus slaptažodžius (24+ simboliai) su didžiosiomis, mažosiomis raidėmis, skaičiais ir simboliais
- Atsiminkite tik 2 slaptažodžius: kompiuterio ir slaptažodžių tvarkyklės

Detaliau:

Slaptažodžių tvarkyklės

Yra du saugūs keliai, išsirink, kuris tau tinka:

A. Offline tvarkyklė (maksimalus privatumas, labiau pažengusiems)

- Kompiuteryje(*tai reiškia, kad nėra saugoma debesyje*): mano rekomenduojama programa **KeePassXC** (Windows/macOS/Linux).
- Telefonuose - tik skaitymui (atsarginė prieiga):
    - Android: **KeePassDX** (galima atidaryti duomenų bazę iš USB-C).
    - iOS: Strongbox (atidaryti failą iš kompiuterio ir nustatai Read-Only).
- Duomenų bazę laikai lokaliai, su atsargine kopija užšifruotame USB.

B. Online tvarkyklė (patogu, sinchronizuoja, kasdieniniam vartotojui)

Yra įvairių slaptažodžių tvarkyklių, paieškoję google galite rasti bent 4 populiarius, bet vienas jų yra kurtas mūsų Lietuvių - **NordPass**!

- Sinchronizacija tarp visų įrenginių, integruota 2FA.
- Patogu ir lengva naudotis kiekvienam vartotojui.
- Galima lengvai dalintis slaptažodžiais su šeimos nariais.
- Tinka daugumai žmonių. Vis tiek generuoji 24+ simbolių slaptažodžius ir įjungi 2FA.

Bet kuri tvarkyklė yra geriau nei jokia. Blogiausia yra laikyti tą patį “protingą” slaptažodį per 20+ paskyrų.

Dviejų faktorių autentifikacija

Ką tai reiškia?
Prisijungimui reikia dviejų skirtingų įrodymų: kažko, ką žinai (slaptažodis), ir kažko, ką turi arba esi (telefonas, raktas, biometriniai duomenys) tokiu atveju yra reikalaujama abiejų duomenų, norint prisijungti prie sistemų. Net jei slaptažodis pavogtas, antras faktorius sustabdo įsilaužėlį.(*Jei antrasis faktorius saugus, o ne SMS*)

Hierarchija nuo geriausio iki blogiausio

1. **FIDO2/U2F saugos raktas** (*YubiKey/OnlyKey/SoloKey*)
    a. Atsparus fišingo atakom, atsparu SIM-swap atakom ir duomenų nutekėjimams.
    b. Rekomenduojama turėti 2 vnt. (pagrindinį + atsarginį).
2. **Passkeys / WebAuth "platforminis autentifikatorius"** (*BIOMETRIKA įrenginyje*)
    a. Biometrija (*Face ID/Touch ID/Windows Hello*) vietoje atrakinimo slaptažodžiu vietiniuose "Secure Enclave/TPM" įrenginiuose kurie integruoti įrenginiuose ir neskleidžiama jų informacija už ribų.
    b. Serveriui keliauja tik kriptografinis įrodymas, ne biometrija.
    c. Saugumas prilygsta FIDO2 raktui, bet priklauso nuo įrenginio ekosistemos.
3. **TOTP (30 s arba kitaip - laikinieji pin)** - atskirai telefone (*Google/Microsoft Authenticator ir pan.*)
    a. Saugiau už SMS, offline, plačiai palaikoma.
    b. Trūkumas: galima pasinaudoji įvykus fišingo atakai (vartotojas gali suvesti kodą netikram puslapiui).
    c. Turint prisijungima prie žmogaus google paketo prieigos - galima gauti pilną priėjimą prie Google Authenticator;
4. **SMS 2FA / skambučiai / el. pašto kodai**
    a. Minimalus saugumas. Pažeidžiama SIM-swap, perėmimo, SS7 atakomis.
    b. Naudoti tik jei nėra kitų pasirinkimų - geriau nei nieko.

Praktiniai pavyzdžiai

Gmail/Google Workspace: FIDO (YubiKey) + TOTP kaip atsarginis. Atsarginį raktą palikti seife.
Bankas: jei palaiko FIDO - naudok; jei ne, TOTP per tvarkyklę.
Socialiniai tinklai - Facebook/Instagram ir kiti: FIDO.
El. parduotuvės/Web Svetainės administravimas (Shopify/WooCommerce): privalomas FIDO arba TOTP; administratoriams - atskiri vartotojai, jokių bendrų paskyrų.

Kodėl FIDO raktas toks stiprus?

Phishing-proof: raktas "pasirašo" prisijungimą tik tikram domenui, net jei paspausi netikrą nuorodą, raktas neveiks.

Nėra kodo, kurį nurašytum, taigi nieko neperduodi apgavikui.
Unikalus atsakymas kiekvienam prisijungimui, klonuoti be fizinio rakto neįmanoma.

Ką nusipirkti?

Praktiškas komplektas yra du YubiKey 5C NFC (USB-C + NFC), arba 5C Nano + 5C NFC. Vieną nešiojiesi, kitą laikai atskirai kaip “draudimą“.

Biometrijos naudojimas

Biometrinė autentifikacija tai technologija, leidžianti patvirtinti jūsų tapatybę pagal jūsų unikalius fizinius požymius. Tai yra saugi autentifikacijos forma, nes jūsų biometriniai duomenys **niekada neišsiunčiami iš įrenginio** ir saugomi tik specialioje apsaugotoje aparatinėje dalyje (Secure Enclave/TPM), **prie kurios negali prieiti net pats gamintojų įrenginys**.

Biometrija (pirštų atspaudai, veido atpažinimas) tampa vis svarbesne apsaugos dalimi:

- **Įrenginio atrakinimas**: naudokite pirštų atspaudus/veidą vietoj PIN
- **Mokėjimai**: Apple Pay, Google Pay su biometrija
- **Programėlių atrakinimas**: bankininkystės, mokesčių programos
- **Passkeys***: naujos kartos prisijungimas vietoj slaptažodžių

* - Passkeys tai naujoviškas prisijungimo būdas, pakeičiantis tradicinius slaptažodžius. Vietoj slaptažodžio įsiminimo, patvirtinate savo tapatybę naudodami biometriją (pirštą ar veidą) savo įrenginyje, kuris saugiai komunikuoja su svetaine ar programėle.

TOTP - vienkartiniai slaptažodžiai

Tai yra laikinasis vienkartinis slaptažodis, kuris generuojamas pagal laiką ir keičiasi kas 30 sekundžių. Tai vienas populiariausių dviejų faktorių autentifikacijos (2FA) metodų, naudojamas kaip papildoma apsauga greta jūsų pagrindinio slaptažodžio.

Specializuotos TOTP autentifikacijos programėles kurias vertėtų naudoti:

- Google Authenticator (Android, iOS)
- Microsoft Authenticator (Android, iOS)
- Authy (Android, iOS, kompiuteryje)

TOTP yra puikus saugumo sluoksnis, nes net jei kas nors sužino jūsų slaptažodį, be laikinojo kodo prisijungti negalės, o šie kodai galioja tik 30 sekundžių ir nuolat keičiasi.

SMS 2FA - naudok protingai

Jei paslauga leidžia tik SMS, palik seną/pakaitinį numerį arba perkelk į VOIP (virtualus numeris). Taip netepsi naujo asmeninio numerio visur.

Patvirtink SMS kodą, bet kuo greičiau pereik prie TOTP/FIDO, jei tik atsiras galimybė. SIM-swap yra reali grėsmė (apgauna operatorių ir perkelia tavo numerį). FIDO/TOTP nuo to nekenčia, SMS - kenčia.

Dažniausios klaidos

Keisti slaptažodžius viešame Wi-Fi - NE. Keisk namuose ar per VPN*(su VPN tavo duomenys šifruojami)*.
Vienas FIDO raktas, jei jį pamesi ar pamirši - neteksi prieigos. Visada turėk du.
TOTP tik telefone be kopijos, o jei prarasi telefoną - prarasi ir OTP. Turėk atsarginę TOTP strategiją.
Bendros administratoriaus paskyros įmonėje - NE, personalizuok kiekvienam skirtingą, FIDO/2FA privaloma.
Tas pats slaptažodis keliose vietose - jei jūsų slaptažodis nutekės į internetą, variantas, kad vienu slaptažodžiu galima bus prieiti prie skirtingų paskyrų.
Lengvai atspėjami slaptažodžiai - vaikų vardai, gimimo datos, "labas123", “nesakysiu”), įsilauželiai panagrinėję jūsų socialinius tinklus, kur dažnai paliekate informacija tiek apie savo gyvūnų vardus tiek gimimo metus gali atspėti ir jūsų slaptažodžius.