

Kaip apsaugoti Facebook ir Instagram paskyras

Deividas Ambrazevičius Oct 15, 2026

Dauguma nulaužimų prasideda ne nuo techninio įsilaužimo, o nuo apgaulės, kai žmogus pats atiduoda prieigą. Socialinė inžinerija užima daugiau nei 70% visų duomenų ir pinigų praradimo atvejų.

Gidas padės išvengti dažniausių nulaužimų: fišingo, netikrų "prekės ženklų" failų, ClickFix ir FileFix atakų bei puslapių perėmimo. O jei bėda jau nutiko, parodys, ką daryti pirmiausia, kad paskyrą atgautum kuo greičiau.

Kaip skaityti: prie kiekvieno žingsnio nurodytas kelias lietuviškame meniu (**LT**) ir angliškame meniu (**EN**). Meta kartais pakeičia meniu pavadinimus. Jei punkto nerandi, nustatymuose naudok paiešką (🔍) ir įvesk raktažodį, pvz., "dviejų veiksmų" / "two-factor".

Pačioje apačioje rasite kontrolinį sąrašą kuriame galėsite laikytis kaip "špargalkę" extra atvejams.

*Tiem kam įdomu ir nori detalesnio ir gilesnio plano apie **skaitmeninį šydą** ir stiprų privatumo lygį jau nuo rytojaus - rekomenduoju mano kurtą gidą kur išmoksite ne tik atpažinti atakas, bet ir gausite konkrečių pavyzdžių kaip kontroliuoti savo skaitmeninę erdvę:*

<https://ambrazevicius.com/skaitmenine-savigyna/>

Kaip vyksta nulaužimai

Penki dažniausi būdai, kuriuos verta atpažinti:

1. **Fišingas "Meta Support" vardu.** Ateina žinutė apie "autorių teisių pažeidimą" arba įspėjimas, kad "puslapis bus ištrintas per 24 val.". Nuoroda veda į netikrą prisijungimo puslapį, kur išvilioja slaptažodį ir 2FA kodą.
2. **Netikri prekės ženklai su failais.** Siūlomas "bendradarbiavimas" ir atsiunčiamas ZIP, RAR ar "PDF" failas. Iš tikrųjų tai kenkėjiška programa (infostealer).
3. **Sesijų vagystė.** Infostealer pavagia naršyklės slapukus (cookies), todėl užpuolikas prisijungia kaip tu, net jei turi 2FA. Tada jis prideda save prie puslapio ir pašalina tave.
4. **ClickFix ir FileFix.** Svetainė su netikra CAPTCHA ar "klaidos taisymu" lieps nukopijuoti komandą ir įklijuoti ją į Windows. Taip įdiegiama ta pati kenkėjiška programa.
5. **Masinis reportinimas.** Botai masiškai reportina paskyrą, ji automatiškai užblokuojama, o tada atsiranda "pagalbininkų", siūlančių atkūrimą už pinigus.

1. Facebook asmeninės paskyros apsauga

Visi šie nustatymai yra **Paskyrų centre (Accounts Center)**, kuris bendras Facebook ir Instagram.

1. Įjunk dviejų veiksmų autentifikavimą (2FA) per programėlę.

- LT: Meniu (☰) → ⚙️ Nustatymai ir privatumas → Nustatymai → Paskyrų centras → Slaptažodis ir sauga → Dviejų veiksmų autentifikavimas
- EN: Menu (☰) → ⚙️ Settings & privacy → Settings → Accounts Center → Password and security → Two-factor authentication
 - i. Pasirink paskyrą ir būdą **"Autentifikavimo programėlė" / "Authentication app"** (reikės atsisiųsti Google Authenticator arba Microsoft Authenticator). **SMS nenaudok** - mažiausiai patikima technologija.

2. Išsisaugok atsarginius kodus.

- LT: Dviejų veiksmų autentifikavimas → Papildomi metodai → Atsarginiai kodai
- EN: Two-factor authentication → Additional methods → Recovery codes
 - i. Nusirašyk ant popieriaus ar pasidaryk nuotrauką ir laikyk saugioje vietoje, ne telefone.

3. Išmesk svetimus įrenginius.

- LT: Paskyrų centras → Slaptažodis ir sauga → Kur esate prisijungę
- EN: Accounts Center → Password and security → Where you're logged in
 - i. Atjunk viską, ko neatpažįsti.

4. Įjunk įspėjimus apie prisijungimą.

- LT: Paskyrų centras → Slaptažodis ir sauga → Įspėjimai apie prisijungimą
- EN: Accounts Center → Password and security → Login alerts
 - i. Įjunk ir programėlės pranešimus, ir el. laiškus.

5. Atlik saugos patikrą.

- LT: Paskyrų centras → Slaptažodis ir sauga → Saugos patikra
- EN: Accounts Center → Password and security → Security Checkup

6. Atjunk nereikalingas programas.

- LT: Nustatymai ir privatumas → Nustatymai → Programos ir svetainės
- EN: Settings & privacy → Settings → Apps and websites
 - i. Pašalink viską, ko nebenaudoji (senus žaidimus, testus, automatizavimo įrankius).

7. Naudok unikalų slaptažodį. Jis turi būti naudojamas tik Facebook. Geriausia jį laikyti slaptažodžių tvarkyklėje (Bitwarden, 1Password, Google Password Manager).

2. Instagram apsauga

Jei Instagram prijungtas prie to paties Paskyrų centro, 2FA ir įrenginiai tvarkomi ten pat. Vis tiek patikrink:

1. 2FA per programėlę.

- LT: Profilis → ☰ → Nustatymai ir veikla → Paskyrų centras → Slaptažodis ir sauga → Dviejų veiksmų autentifikavimas

- EN: Profile → ☰ → Settings and activity → Accounts Center → Password and security → Two-factor authentication
- 2. **Kur esi prisijungęs.**
 - LT: Paskyrų centras → Slaptažodis ir sauga → Kur esate prisijungę
 - EN: Accounts Center → Password and security → Where you're logged in
- 3. **Prijungtos programos.**
 - LT: Nustatymai ir veikla → Svetainės leidimai → Programos ir svetainės
 - EN: Settings and activity → Website permissions → Apps and websites
 - i. Palik tik tuos įrankius, kuriuos tikrai naudoji. Kiekvienas prijungtas įrankis yra papildoma prieiga.
- 4. **Patikrink Meta laiškus.**
 - LT: Nustatymai ir veikla → Paskyrų centras → Slaptažodis ir sauga → Naujausi el. laiškai
 - EN: Settings and activity → Accounts Center → Password and security → Recent emails
 - i. Čia matai visus tikrus Instagram laiškus. Jei laiško čia nėra, jis netikras.

3. Facebook puslapio ir verslo apsauga

Visišką valdymą turėtum turėti tik du žmonės: tu ir vienas patikimas žmogus su tikra paskyra ir įjungtu 2FA. Kiekvienas papildomas administratorius yra dar viena galimybė įsilaužti.

1. **Patikrink, kas turi prieigą prie puslapio.**
 - LT: Perjunk į puslapį → Meniu → Nustatymai → Puslapio nustatymai → Puslapio prieiga
 - EN: Switch to Page → Menu → Settings → Page setup → Page access
 - i. Pašalink nepažįstamus. Kitiems vietoj visiško valdymo duok tik dalinę prieigą (pvz., turinio kūrimui).
2. **Puslapį perkelk į verslo portfolio.**
 - Naršyklėje atsidaryk business.facebook.com ir susikurk verslo portfolio (Business portfolio).
 - LT: Verslo nustatymai → Paskyros → Puslapiai → Pridėti
 - EN: Business settings → Accounts → Pages → Add
 - i. Taip pat pridėk ir Instagram paskyrą (Accounts → Instagram accounts).
3. **Padaryk 2FA privalomą visiems.**
 - LT: Verslo nustatymai → Saugos centras → Dviejų veiksmų autentifikavimas → Visi
 - EN: Business settings → Security Center → Two-factor authentication → Everyone
4. **Patikrink žmonių sąrašą versle.**
 - LT: Verslo nustatymai → Vartotojai → Žmonės
 - EN: Business settings → Users → People
 - i. Ištrink visus, kurių neatpažįsti, ir nepriimtus senus kvietimus.
5. **Puslapio pranešimus skaityk tik oficialiose vietose.**

- LT: Puslapis → Paskyros būseną ir Palaikymo dėžutę
 - EN: Page → Account Status and Support Inbox
 - i. Meta niekada nerašo per Messenger ar DM apie pažeidimus ar puslapio ištrynimą.
6. **Svarbu: netikras antras profilis kaip "atsarginis administratorius" pažeidžia Meta taisykles. Meta tokias paskyras blokuoja, ir tai gali paliesti tavo puslapį. Antras administratorius turi būti tikras žmogus.**

4. El. pašto apsauga

Kas valdo tavo el. paštą, tas gali atkurti ir Facebook bei Instagram. Todėl el. paštas turi būti apsaugotas taip pat gerai.

1. **Ijunk patvirtinimą dviem veiksmais Gmail.**
 - Atsidaryk myaccount.google.com/security
 - LT: Sauga → Patvirtinimas dviem veiksmais
 - EN: Security → 2-Step Verification
 - i. Geriausia rinktis "Slaptažodžių raktą" (Passkey) arba Google Authenticator.
2. **Atlik saugos patikrą.**
 - LT: Sauga → Saugos patikra
 - EN: Security → Security Checkup
3. **Patikrink peradresavimą.** Nulaužus paštą, kartais nustatoma, kad laiškai slapta keliautų kitur.
 - LT: Gmail →  Nustatymai → Žiūrėti visus nustatymus → Peradresavimas ir POP / IMAP
 - EN: Gmail →  Settings → See all settings → Forwarding and POP/IMAP
4. **Turink atskirą el. paštą tik Meta paskyroms.** Niekur kitur juo nesiregistruok ir niekam jo neduok.

5. ClickFix ir FileFix: kaip atpažinti ir apsisaugoti

Auksinė taisyklė: jokia tikra svetainė, CAPTCHA ar "patikrinimas, kad nesi robotas" niekada neprašo nieko kopijuoti ir įklijuoti į kompiuterį.

Kaip atrodo

- **ClickFix:** svetainė rodo netikrą CAPTCHA arba "klaidą" ir lieps paspausti **Win + R**, tada **Ctrl + V** ir **Enter**. Komanda jau būna slapta nukopijuota į tavo iškarpinę.
- **FileFix:** svetainė sako, kad "failas bendrinamas su tavimi", ir lieps atidaryti **Failų naršyklę (File Explorer)** bei įklijuoti "kelį iki failo" į adreso juostą. Iš tikrųjų tai komanda.
- **Mac versija:** lieps atidaryti **Terminalą** ir įklijuoti komandą.

Kaip apsisaugoti

1. Jei svetainė lieps spausti Win + R, atidaryti Terminalą ar įklijuoti ką nors į File Explorer, **iškart uždaryk skirtuką.**
2. Puslapį valdyk atskirame naršyklės profilyje arba visiškai atskiroje naršyklėje ("švari zona"), kuriame nėra plėtinių ir kuriame nieko nesisiunti.
3. Klientų ir "prekės ženklų" failus peržiūrėk tik per Google Drive, jų nesisiųsdamas.
4. Laikyk įjungtą Windows saugą (Windows Security) ir atnaujink sistemą.

Jei jau įklijavai komandą

1. Atjunk kompiuterį nuo interneto (Wi-Fi ir laidą).
2. **Iš kito įrenginio** (pvz., telefono) pakeisk Facebook, Instagram ir el. pašto slaptažodžius ir atjunk visas sesijas.
3. Paleisk gilų nuskaitymą:
 - LT: Windows sauga → Apsauga nuo virusų ir grėsmių → Nuskaitymo parinktys → "Microsoft Defender" autonominis nuskaitymas
 - EN: Windows Security → Virus & threat protection → Scan options → Microsoft Defender Offline scan
4. Jei kompiuteris buvo naudojamas bankininkystei ar kriptovaliutoms, rimtai svarstyk Windows perdiegimą ir kreipkis į IT specialistą.

6. Jei paskyra ar puslapis jau perimti

Veik per pirmas valandas: kuo greičiau, tuo didesnė tikimybė atgauti.

1. **Ieškok laiško nuo security@facebookmail.com.** Jame būna nuoroda, kuri leidžia atšaukti pakeitimus ("Tai buvau ne aš" / "This wasn't me" arba "let us know").
2. **Naudok oficialius atkūrimo puslapius:** facebook.com/hacked ir instagram.com/hacked. Instagram dažnai siūlo vaizdo selfio patikrą.
3. **Jei prarastas tik puslapis:** kitas administratorius per business.facebook.com pašalina įsilaužėlį ir vėl tave prideda.
4. **Pakeisk slaptažodžius ir atjunk visas sesijas** (žr. 1 ir 4 skyrius). Jei įtari kenkėjišką programą, tai daryk iš kito įrenginio.
5. **Perspėk sekėjus** per asmeninį profilį ir Instagram story, kad nepasitikėtų puslapio žinutėmis ir įrašais.
6. **Jei paskyra užblokuota dėl reportinių:** teik apeliaciją per oficialią formą ir nekurk naujų paskyrų.
7. **Niekam nemokėk už "atkūrimą".** Tokie "hakeriai-pagalbininkai" beveik visada yra sukčiai.
8. **Pranešk policijai** per e-policija.lt. Tai naudinga dokumentacijai ir tolesniems veiksams.
9. **Svarbioms paskyroms** apsvarstyk Meta Verified prenumeratą, kuri suteikia prieigą prie gyvo palaikymo.

Kontrolinis sąrašas

- 2FA per programėlę įjungtas Facebook ir Instagram
- Atsarginiai kodai išsaugoti ne telefone
- Svetimi įrenginiai atjungti, įspėjimai apie prisijungimą įjungti
- Nereikalingos programos atjungtos
- Puslapis perkeltas į verslo portfolio
- Visišką valdymą turi tik 2 tikri žmonės su 2FA
- Versle 2FA privalomas visiems
- El. paštas apsaugotas 2FA, peradresavimas patikrintas
- Visur unikalūs slaptažodžiai
- Žinau: jokia svetainė neliepia nieko įklijuoti į kompiuterį
- Žinau: Meta nerašo per DM apie pažeidimus
- Išsisaugojau facebook.com/hacked ir instagram.com/hacked

Ką patikrinti per 5 minutes DABAR

Facebook ir Instagram saugumo patikra. Padaryk tai šiandien, kol niekas nenutiko.

1

Ar įjungtas 2FA per programėlę?

Pasirink „Autentifikavimo programėlė“ (Google ar Microsoft Authenticator), ne SMS. Išsisaugok atsarginius kodus ant popieriaus.

LT: Facebook: Meniu (☰) → Nustatymai ir privatumas → Nustatymai → Paskyrų centras → Slaptažodis ir sauga → Dviejų veiksmų autentifikavimas

EN: Facebook: Menu (☰) → Settings & privacy → Settings → Accounts Center → Password and security → Two-factor authentication

2

Ar nėra svetimų įrenginių?

Atjunk viską, ko neatpažįsti. Ten pat įjunk įspėjimus apie naujus prisijungimus.

LT: Paskyrų centras → Slaptažodis ir sauga → Kur esate prisijungę / Įspėjimai apie prisijungimą

EN: Accounts Center → Password and security → Where you're logged in / Login alerts

3

Kas valdo tavo puslapį?

Visišką valdymą turėtų turėti tik 2 tikri, pažįstami žmonės. Nepažįstamus pašalink iš karto.

LT: Perjunk į puslapį → Nustatymai → Puslapio nustatymai → Puslapio prieiga

EN: Switch to Page → Settings → Page setup → Page access

4

Ar el. paštas apsaugotas?

Kas valdo el. paštą, tas gali atkurti ir Facebook. Įjunk 2FA ir patikrink, ar laiškai niekur slapta neperadresuojami.

LT: myaccount.google.com/security → Patvirtinimas dviem veiksmais; Gmail → Nustatymai → Peradresavimas ir POP / IMAP

EN: myaccount.google.com/security → 2-Step Verification; Gmail → Settings → Forwarding and POP/IMAP

5

Kokios programos prijungtos?

Kiekviena prijungta programa ar įrankis yra papildomas kelias į paskyrą. Palik tik tas, kurias tikrai naudoji.

LT: Facebook: Nustatymai → Programos ir svetainės; Instagram: Nustatymai ir veikla → Svetainės leidimai

EN: Facebook: Settings → Apps and websites; Instagram: Settings and activity → Website permissions

3 taisyklės, kurias verta įsiminti:

- Meta **niekada** nerašo per Messenger ar DM, kad tavo puslapis bus ištrintas.
- Jokia svetainė ar CAPTCHA **niekada** neprašo spausti Win + R ar ką nors įklijuoti į kompiuterį (ClickFix / FileFix).
- Nesisisųsk failų iš „prekės ženklų“ ar „klientų“. Peržiūrėk juos tik naršyklėje.

Ką daryti, kai NULAUŽĖ

Veik per pirmas valandas. Kuo greičiau, tuo didesnė tikimybė viską atgauti.

1

Rask laišką nuo security@facebookmail.com

Facebook siunčia laišką apie kiekvieną svarbų pakeitimą. Jame yra nuoroda „Tai buvau ne aš“ / „let us know“, kuri leidžia atšaukti pakeitimus. Patikrink ir „Šlamšto“ aplanką.

2

Eik į oficialų atkūrimo puslapį

Įvesk naršyklėje ranka, o ne per nuorodas žinutėse. Instagram dažnai pasiūlo vaizdo selfio patikrą.

LT: facebook.com/hacked • instagram.com/hacked

3

Atjunk visas sesijas ir pakeisk slaptažodžius

Pakeisk Facebook, Instagram ir el. pašto slaptažodžius. Jei neseniai ką nors atsisaiuntei ar įklijavai komandą, tai daryk **iš kito įrenginio** (telefono), nes kompiuteris gali būti užkrėstas.

LT: Paskyrų centras → Slaptažodis ir sauga → Kur esate prisijungę → Atsijungti

EN: Accounts Center → Password and security → Where you're logged in → Log out

4

Prarastas tik puslapis? Naudok antrą administratorių

Jei tavo profilis veikia, bet tave išmetė iš puslapio, kitas administratorius gali pašalinti įsilaužėlį ir vėl tave pridėti.

LT: business.facebook.com → Verslo nustatymai → Vartotojai → Žmonės

EN: business.facebook.com → Business settings → Users → People

5

Patikrink el. paštą

Ar nepakeistas atsarginis el. paštas ar telefonas, ar nėra peradresavimo taisyklių, ar nėra svetimų prisijungimų.

LT: myaccount.google.com → Sauga → Naujausia saugos veikla

EN: myaccount.google.com → Security → Recent security activity

6

Perspėk sekėjus

Per asmeninį profilį ir Instagram story parašyk, kad puslapis perimtas ir nereikia pasitikėti jo žinutėmis, nuorodomis ar prašymais pervesti pinigų.

7

Pranešk policijai

Pareiškimą pateik per e-policija.lt. Tai padės dokumentuoti įvykį ir gali būti naudinga atkuriant paskyrą.

Niekam nemokėk už „atkūrimą“. Žmonės, kurie po tavo įrašais ar žinutėse siūlo „atgauti paskyrą už pinigus“, beveik visada yra sukčiai, o kartais tie patys įsilaužėliai. Paskyra atkuriam tik per oficialius Meta kanalus.