

2FA – Dvo Faktorska Autentikacija

1. Što je 2FA (Dvo faktorska autentikacija)

Dvostruka autentikacija je sigurnosni process koji prilikom prijave u aplikaciju od korisnika zahtijeva autentikaciju na dvije različite razine. Ovime se omogućuje dodatna razina sigurnosti u aplikaciji.

2. Jeli 2FA obavezna ili opcionalna?

Dvostruka autentikacija će biti **obavezna** za sve korisničke račune u domeni Sveučilišta Sjever, što znači da od 17.02.2025 godine (ponedjeljak) morate posložiti sve prema uputama.

3. Koja metoda autentikacije je potrebna?

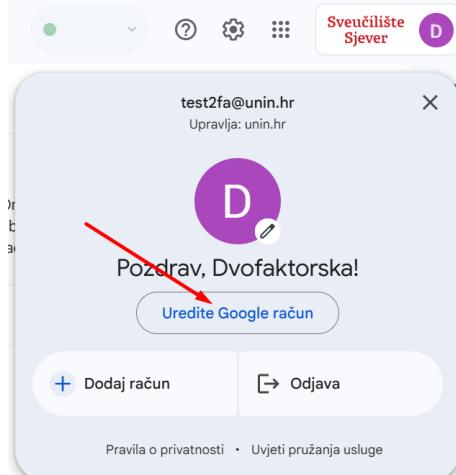
Google nudi više načina autentikacije, najbolja opcija je da se instalira Google Authenticator kojega možete preuzeti na Vašim mobilnim uređajima sa Android stora ili iOS stora.

UPUTE za postavljanje 2FA:

1. Otvorite Google Račun te kliknite na:



2. Zatim odaberite: "Upravljam svojim google računom" ili "Uredite Google račun"



3. Sljedeći korak je na lijevoj strani izbornika odabrati "Sigurnost"



4. Kada se otvorí stranica postavki za Sigurnost, potrebno je kliknuti na "Potvrda u dva koraka":

A screenshot of the 'Sigurnost' (Security) settings page. The title 'Sigurnost' is at the top, followed by the subtitle 'Postavke i preporuke za zaštitu vašeg računa'. The first section is titled 'Imate sigurnosne preporuke' (You have security recommendations) with a sub-subtitle 'Preporučene radnje pronađene su na stranici Sigurnosna provjera'. It features an icon of a smartphone with a lock and a shield with an exclamation mark. Below this is a blue button 'Zaštitite svoj račun'. The next section is titled 'Nedavna sigurnosna aktivnost' (Recent security activity) with the sub-subtitle 'Nema sigurnosnih aktivnosti ili upozorenja unatrag 28 dana.' The final section is titled 'Način prijave na Google' (Sign-in method for Google) with the sub-subtitle 'Redovito ažurirajte ove podatke da biste uvijek mogli pristupiti svojem Google računu'. It lists four items: 'Potvrda u dva koraka' (Two-step verification), 'Zaporka' (Password), 'Preskoči zaporku kad je moguće' (Skip password when possible), and 'E-adresa za oporavak' (Email for recovery). The 'Potvrda u dva koraka' item has a red arrow pointing to it from the bottom right.

5. Zatim kada se otvori Potvrda u dva koraka, potrebno je prvo odabrati "Autentifikator":

← Potvrda u dva koraka

Uključite potvrdu u dva koraka

Pomoću dodatnog sloja zaštite sprječite hakere da pristupaju vašem računu.

Ako se ne prijavljujete pomoću pristupnog ključa, od vas će se tražiti da izvršite najsigurniji drugi korak dostupan na vašem računu. Druge korake i opcije prijave uvijek možete ažurirati u postavkama. [Otvorite sigurnosne postavke](#)



[Uključite potvrdu u dva koraka](#)

Drugi koraci

Redovito ažurirajte podatke i dodajte više opcija za prijavu da biste mogli pristupiti svojem Google računu

- | | | | | | |
|--|--|--|------------------------------|---------------------------------------|---|
| | Pristupni ključevi i sigurnosni ključevi | | Dodavanje sigurnosnog ključa | > | |
| | Googleova obavijest | | | > | |
| | Autentifikator | | | Dodajte aplikaciju za autentifikaciju | > |
| | Telefonski broj | | | Dodajte broj telefona | + |

6. Zatim pratite upute kako preuzeti aplikaciju sa Trgovine Google play ili iOS APP store:

← Aplikacija Autentifikator

Umjesto da čekate SMS-ove, preuzmte kontrolne kode u aplikaciji za autentifikaciju. To funkcioniра čak i kad telefon nije povezan s internetom.

Najprije preuzmte Google autentifikator u [Trgovini Google Play ili iOS App Storeu.](#)



[+ Postavite autentifikator](#)

NAKON što instalirate aplikaciju autentifikator, kliknite POSTAVI AUTENTIFIKATOR

- 7. Zatim na Vašem uređaju otvorite aplikaciju Google Autentifikator te kliknite na + i odaberite "Skeniraj QR kod" ili "SCAN a QR KOD"**

Postavite aplikaciju autentifikatora

- U aplikaciji Google autentifikator dodirnite +
- Odaberite **Skenirajte QR kôd.**



[Ne možete ga skenirati?](#)

[Odustani](#) [Dalje](#)

Kada ste skenirali QR kod, aplikacija će Vam izbaciti šestero znamenkasti broj, tada je potrebno kliknuti "Dalje" gdje će Vas da unesete taj šestero znamenkasti broj, I kliknite POTVRDI:

Postavite aplikaciju autentifikatora

Unesite šesteroznamenkasti kôd prikazan u aplikaciji

Unesite kôd

[Natrag](#)

[Odustani](#) [Potvrdi](#)

8. Nakon što potvrdite, potrebno je uključiti potvrdu u dva koraka:

← Aplikacija Autentifikator

Uključite potvrdu u dva koraka
Da biste se prijavili pomoću aplikacije za autentifikaciju, uključite potvrdu u dva koraka.

Uključi

Umjesto da čekate SMS-ove, preuzmite kontrolne kodove u aplikaciji za autentifikaciju. To funkcioniра čak i kad telefon nije povezan s internetskom mrežom.

Najprije preuzmite Google autentifikator u [Trgovini Google Play ili iOS App Storeu](#).

Vaš autentifikator

Autentifikator
Dodano upravo sada

[Promijenite aplikaciju autentifikatora](#)

← Potvrda u dva koraka

Uključite potvrdu u dva koraka

Pomoću dodatnog sloja zaštite spriječite hakere da pristupaju vašem računu.

Ako se ne prijavljujete pomoću pristupnog ključa, od vas će se tražiti da izvršite najsigurniji drugi korak dostupan na vašem računu. Druge korake i opcije prijave uvijek možete ažurirati u postavkama. [Otvorite sigurnosne postavke](#)



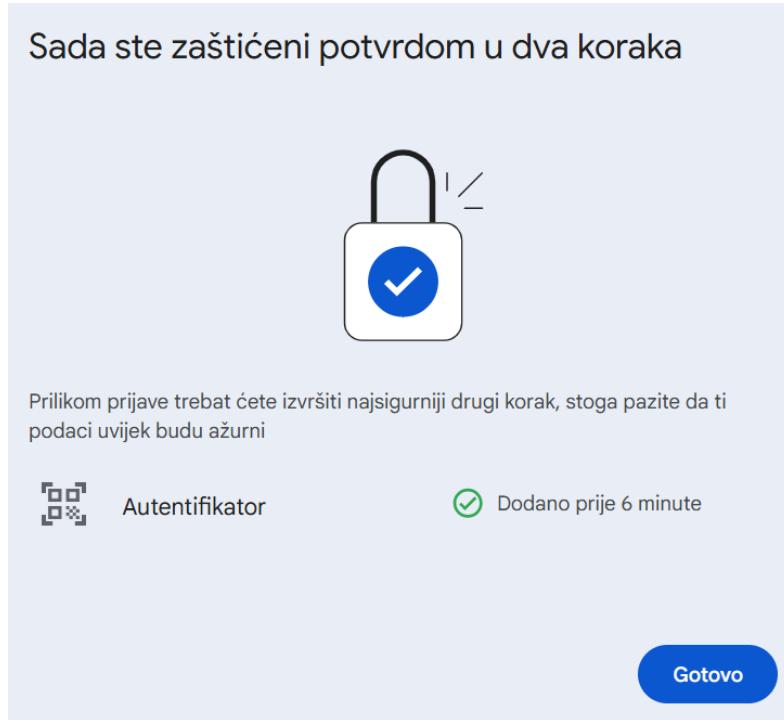
Uključite potvrdu u dva koraka

Drugi koraci

Redovito ažurirajte podatke i dodajte više opcija za prijavu da biste mogli pristupiti svojem Google računu

Pristupni ključevi i sigurnosni ključevi	Dodavanje sigurnosnog ključa	>
Googleova obavijest		>
Autentifikator	Dodano prije 6 minute	>
Telefonski broj	Dodajte broj telefona	+

Te klikom na Uključite potvrdu u dva koraka se pojavljuje sljedeća stranica:



9. Vratite se na Google Račun – SIGURNOST kako bi provjerili da je aktivna, te odaberite VAŠI UREĐAJI kako bi odjavili Vaš korisnički račun sa svih uređaja koji su Vam nepoznati.

The screenshot shows the "Način prijave na Google" (Sign-in method) section. It lists several methods: "Potvrda u dva koraka" (Two-step verification), "Zaporka" (Password), "Preskoči zaporku kad je moguće" (Skip password when possible), "Autentifikator" (Authenticator), "E-adresa za oporavak" (Recovery email), and "Dodata e-adresu" (Add recovery email). The first two items are highlighted with red boxes. Below this, there are sections for "Vaši uređaji" (Your devices) and "Vaše veze s aplikacijama i uslugama trećih strana" (Your connections with apps and services from third parties). The "Vaši uređaji" section shows "1 sesija na Windows računalu" (Windows session) and a "Pronadi izgubljeni uređaj" (Find lost device) button. The "Vaše veze" section has a "Pogledajte sve veze" (View all connections) button. Both sections are also highlighted with red boxes.

NAPOMENA: Prijedlog Sveučilišta Sjever je da se koristi Google autentifikator aplikacija, ukoliko stavite da Vam je dvofaktorska zaštita email, koji je moguće ukraden onda to nije baš najbolja zaštita, a kada Vi imate na svome mobilnom uređaju autentifikator te morate potvrditi prijavu.