

## MFA (MULTI-FACTOR AUTHENTICATION)

Na UL FKKT uvajamo 2 faktorsko avtentikacijo (2FA, MFA). Vse z namenom, da zagotovimo višjo raven varnosti svojih digitalnih identitet ter posledično poslovno informacijskih sistemov. MFA vam zaščiti vašo identiteto, vaše delo, e-maile, Studis, Moodle tudi v primeru kraje vašega gesla, na koncu pa vse to varuje naš skupni sistem.

Za 2- faktorsko avtentikacije boste potrebovali vzpostaviti dva možna načina dodatnega preverjanja vaše identitete. Lahko izbirate med naslednjimi:

1. Microsoftova aplikacija Microsoft Authenticator, ki jo namestite na svojo pametno mobilno napravo (priporočeno je, da je to eden od dveh načinov)
2. Svojo mobilno telefonsko številko, na katero boste prejeli klic in s pritiskom na tipko “#”, potrdili svojo identiteto ali pa boste prejeli enkratno kodo za vpis
3. Svojo službeno številko stacionarnega telefona, na katero boste prejeli klic in z pritiskom na tipko “#”, potrdili svojo identiteto
4. Uporabite kateri koli drug OTP (One-Time-Password, namenski program za enkratno geslo) generator, spodaj so pripeta navodila za enega od njih, ki ga lahko namestite na služben računalnik

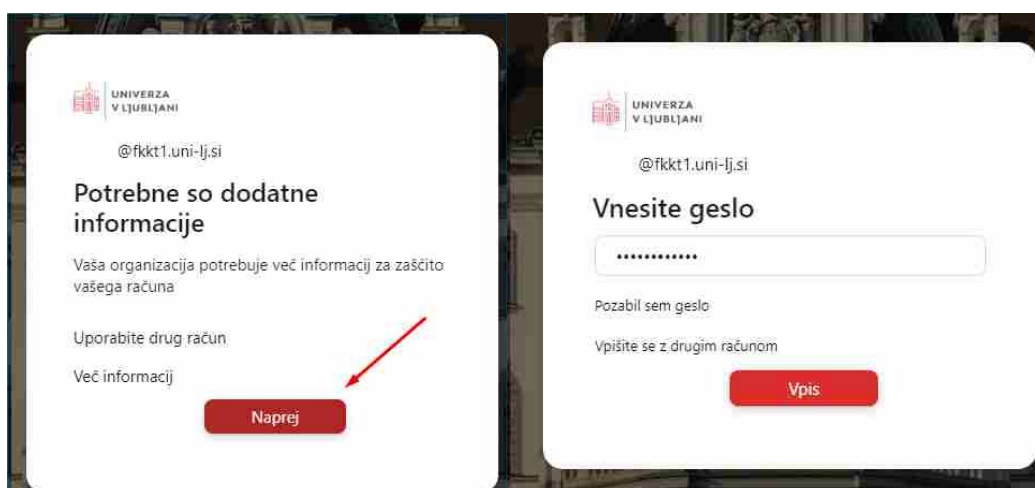
Sistem vas sam lepo vodi skozi nastavitve, tako da le sledite navodilom, ki vam jih sistem prikaže na zaslonu. Med različnimi načini izbirate tako, da v spodnjem levem kotu okna, ki je prikazan na sliki spodaj pritisnete “Želim nastaviti drugačen način”.

Če imate pomisleke pri uporabi lastne naprave za potrebe MFA, vam preostaneta načina 3 in 4, pri čemer pri načinu 4 uporabite generator OTP, nameščen na službeni napravi.

Podrobna uporabniška navodila za vzpostavitev MFA **z zaslonskimi slikami so spodaj.**

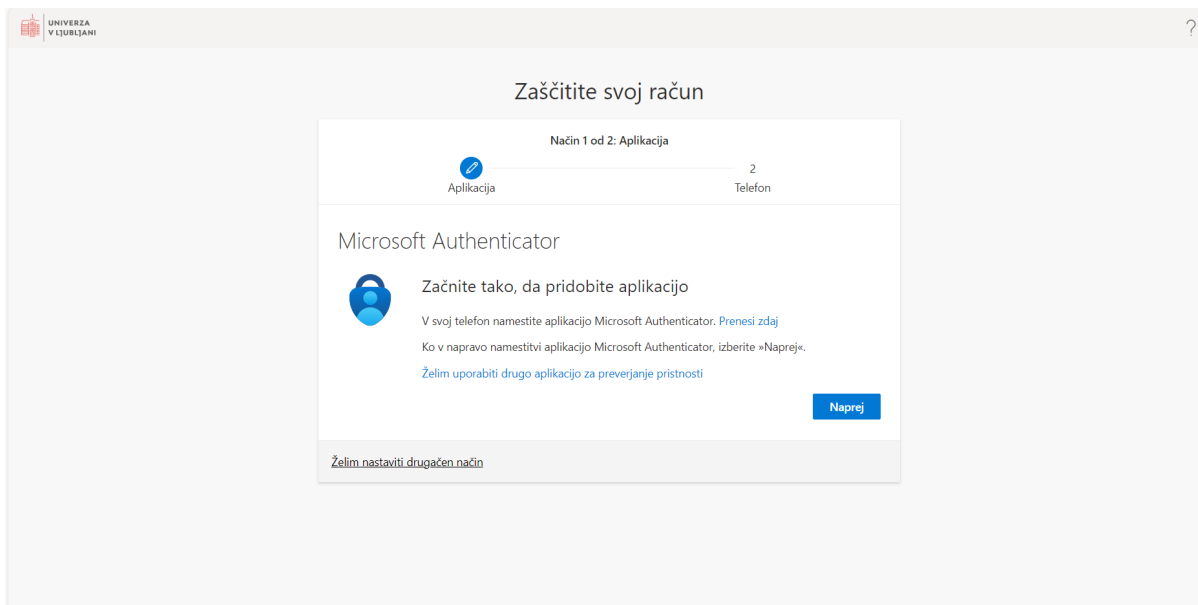
Ko se bo vklopila MFA, se vam bo na zaslonu prikazala zahteva po vpisu gesla.

Vpišite svoje geslo.



# Microsoft Authenticator

## [Aplikacija Microsoft Authenticator za mobilne telefone | Microsoftova varnost](#)



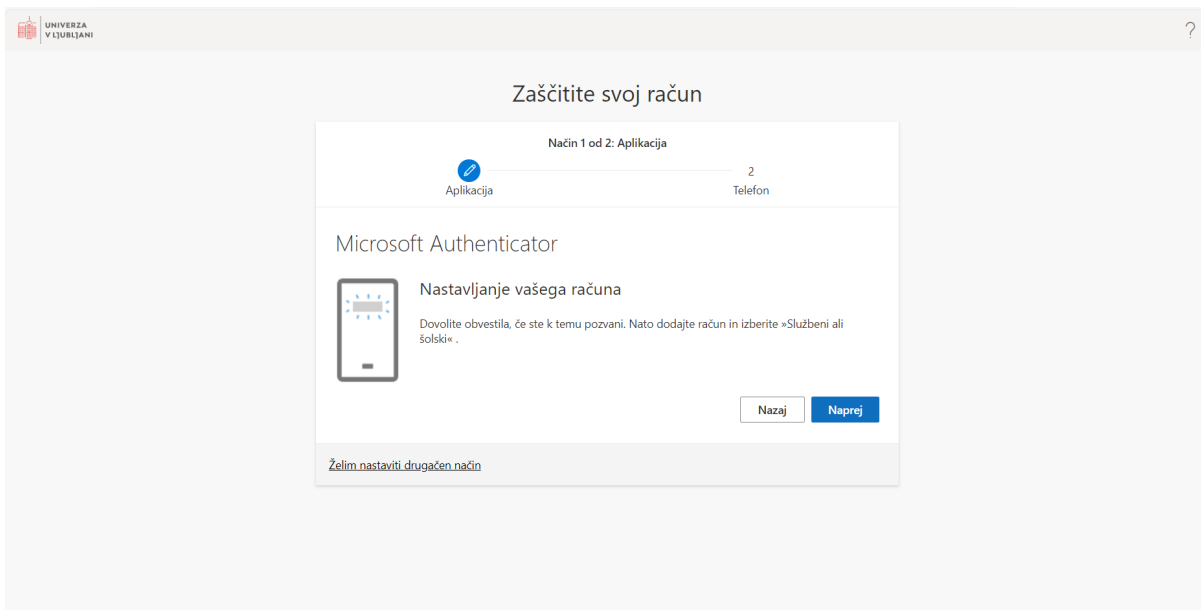
V pomoč sta spodaj kodi za na namestitev.

## [Aplikacija Microsoft Authenticator za mobilne telefone | Microsoftova varnost](#)

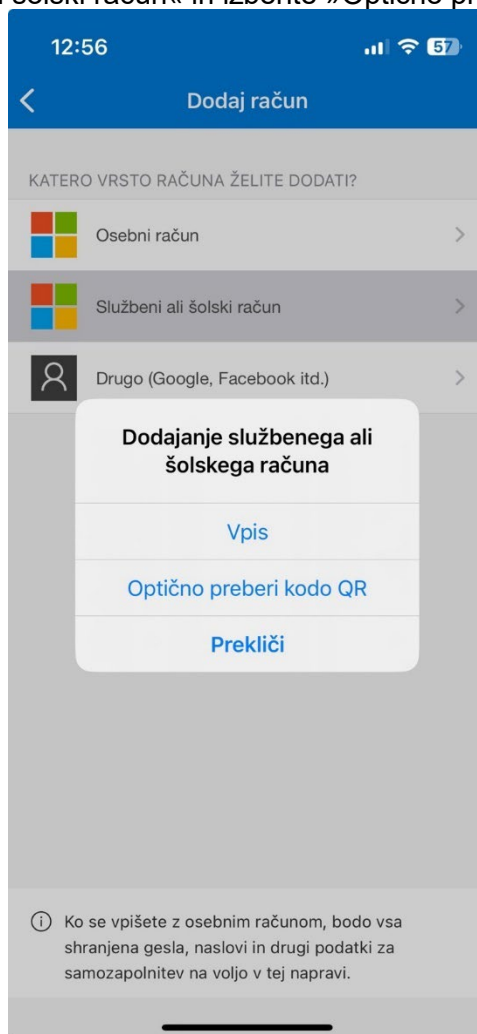
Optično preberite kodo QR z mobilno napravo s sistemom Android ali iOS.



Po namestitvi namenskega programa je treba upariti račun O365 Microsoft z napravo.



Tukaj izberete »Službeni ali šolski račun« in izberite »Optično preberi kodo QR«.



## Skeniraj dobljeno QR kodo

### Microsoft Authenticator

#### Optično preberite kodo QR

Uporabite aplikacijo Microsoft Authenticator in optično preberite kodo QR. S tem boste aplikacijo Microsoft Authenticator povezali s svojim računom.

Ko optično preberete kodo QR, izberite »Naprej«.

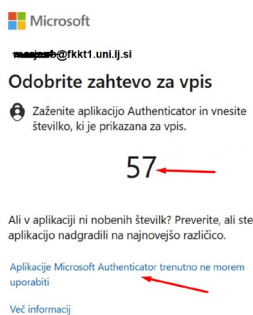


Ali ne morete optično prebrati slike?

Nazaj

Naprej

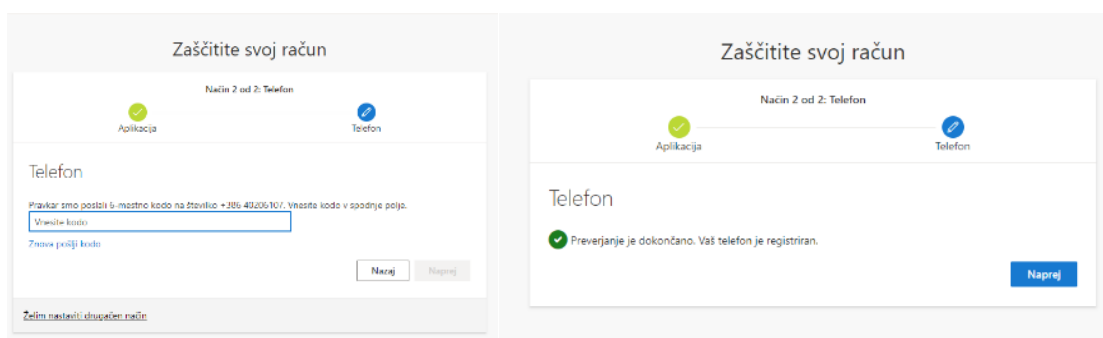
Po uspešni namestitvi, vas bodo sistemi občasno zaprosili, da na telefonu vtipkate številko, ki vam jo prikažejo na zaslonu računalnika. S tem potrdite, da ste to res vi, in ne nekdo, ki ve vaše geslo

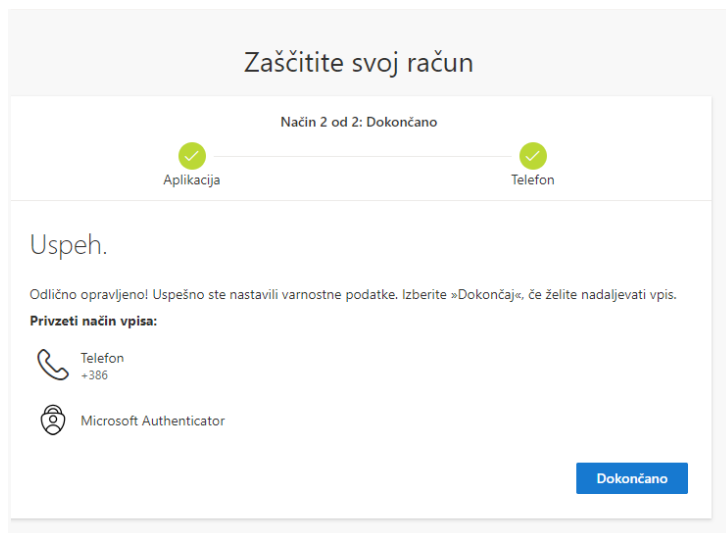


Aplikacija vas bo pozvala k vpisu telefonske številke, ki je lahko za primer klica tudi stacionarni telefon.

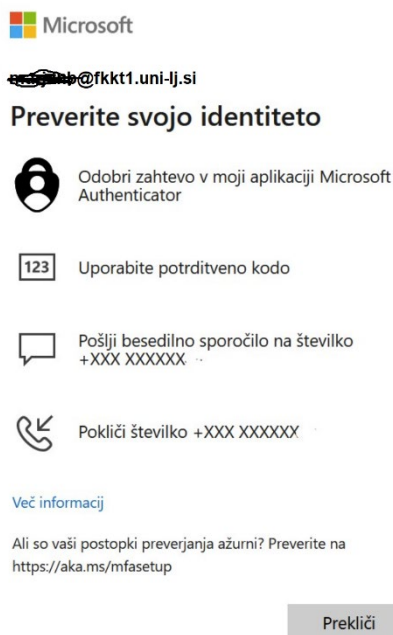
Po potrditvi boste prejeli klic ali SMS-sporočilo, odvisno kaj ste predhodno izbrali za potrditev.

V primeru klica se nanj odzovete in po navodilih pritisnete tipko »#«.





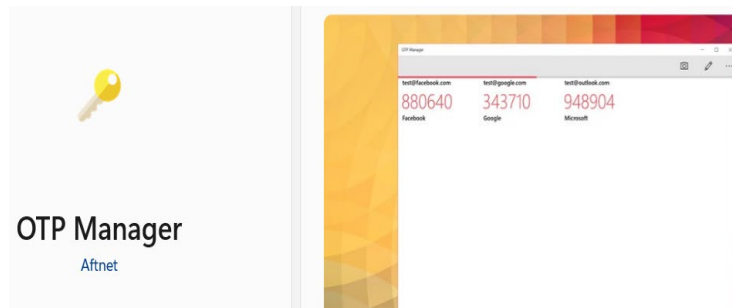
Če namenskega programa ne morete uporabiti, s klikom na "Aplikacije Microsoft Avtenticator trenutno ne morem uporabiti" izberete enega od vaših alternativnih sporočanj kode, ki ste jih tudi morali nastaviti pri vzpostavitvi MFA



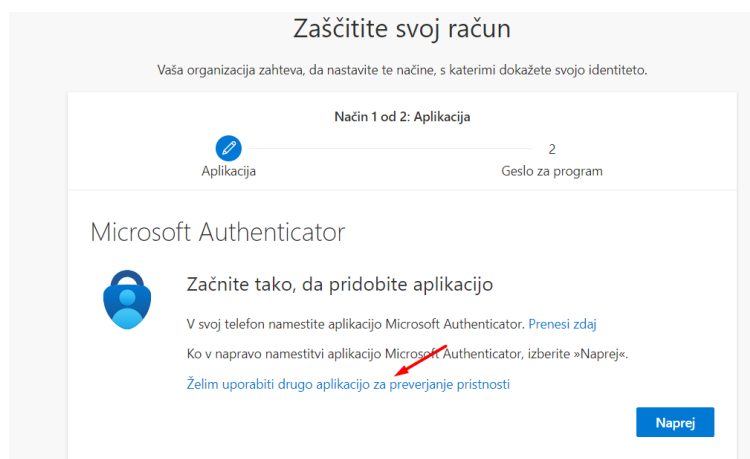
## Za 2FA (MFA) dostop lahko izberemo lahko tudi OTP manager

Z Microsoft strani prenesemo OTP Manager aplikacijo

<https://apps.microsoft.com/detail/9nblggh6hngn?hl=en-us&gl=US>



Ko se prijavimo za nastavev 2FA, izberimo, da želimo uporabiti drugo aplikacijo za preverjanje pristnosti



Izberemo, »ali ne morate optično prebrati slike?« , da dobimo skrivni ključ.

# Aplikacija Authenticator

## Optično preberite kodo QR

Uporabite aplikacijo za preverjanje pristnosti in optično preberite kodo QR. S tem boste aplikacijo za preverjanje pristnosti povezali s svojim računom.

Ko optično preberete kodo QR, izberite »Naprej«.



Ali ne morete optično prebrati slike?

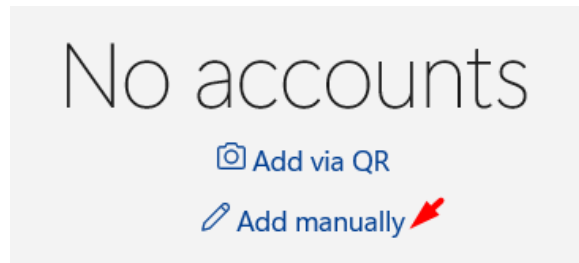
Vnesite te podatke v svojo aplikacijo:

**Ime računa:**



**Skrivni ključ:** dkptrrfgzld5pvq6 

V aplikaciji OTP manager rečemo pri accounts add manually

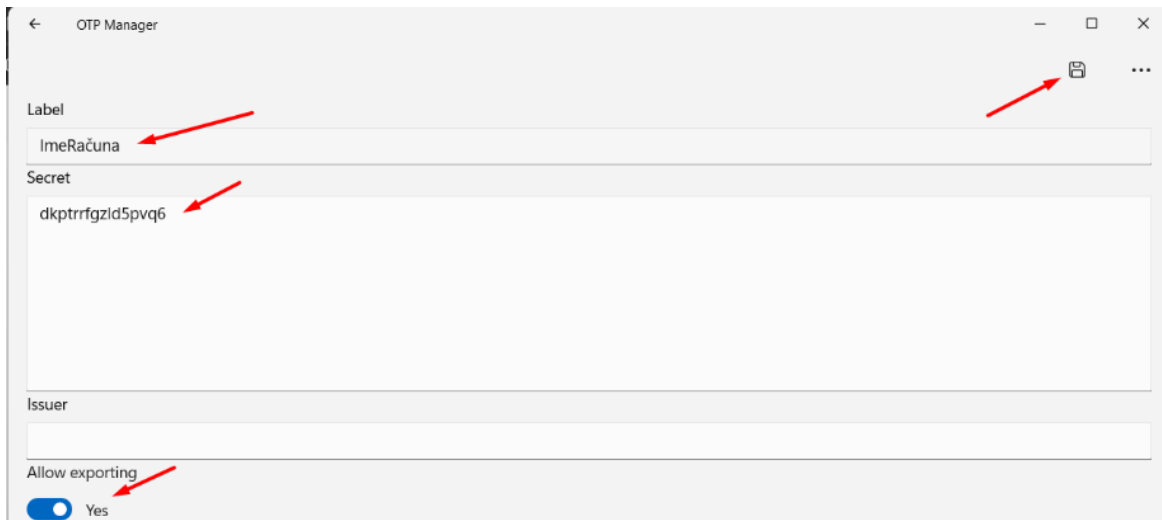


V Label dodamo ime računa ali nekaj prepoznavnega, da bomo vedeli za katero stvar je ta koda

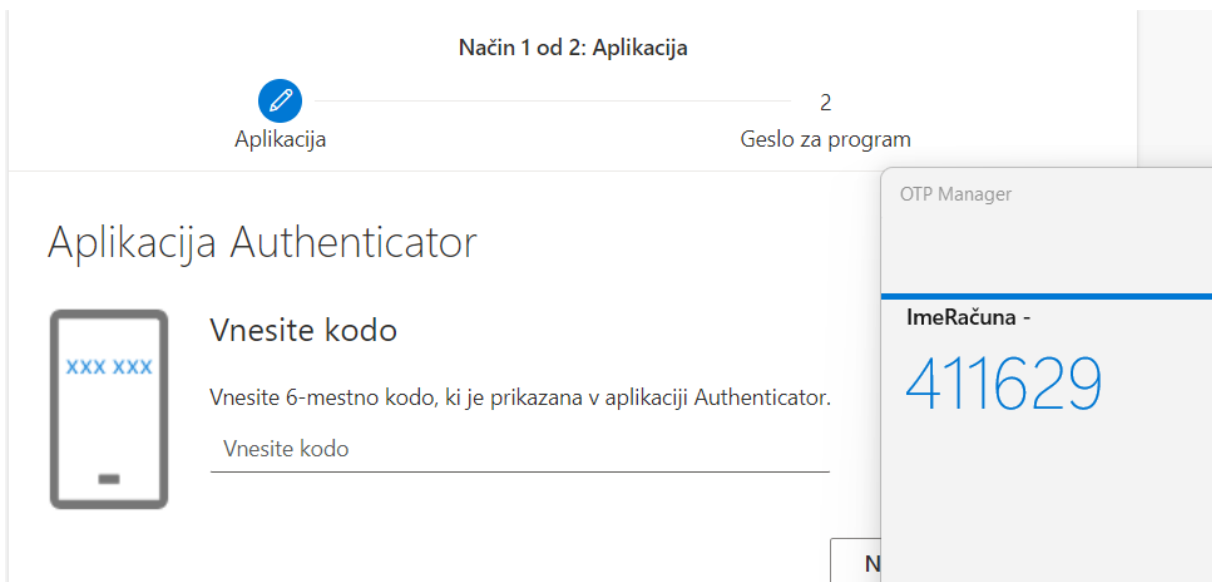
V »secret« prepišemo skrivni ključ

Označimo allow exporting

Kliknemo shrani (disketo)



Kodo, ki jo dobimo potem, prepíšemo v nastavitve 2FA in s tem zaključimo postopek.



Po tem imate vklopljeno 2FA in je račun zaščiten. Prijavo potrjujemo s prepisom števil iz managerja OTP.



Preverjanje možnosti vpisa: <https://mysignins.microsoft.com/security-info>






## Varnostni podatki

To so načini, ki jih uporabljate za vpis v svoj račun ali ponastavitev gesla.

**Privzeti način vpisa:** Microsoft Authenticator – obvestilo [Spremeni](#)

Možnost spreminjanja načina vpisa

+ Dodajte način za vpis.

 Telefon	+386 [redacted]	<a href="#">Spremeni</a>	<a href="#">Izbriši</a>	▼
 Službeni telefon	+386 [redacted]	<a href="#">Spremeni</a>	<a href="#">Izbriši</a>	
 Geslo	Nazadnje posodobljeno: pred 5 meseci	<a href="#">Spremeni</a>		
 Microsoft Authenticator Potisno večkratno preverjanje pristnosti (MFA)	SM-G990B		<a href="#">Izbriši</a>	
 Aplikacija Authenticator Časovno omejeno enkratno geslo (TOTP)			<a href="#">Izbriši</a>	

Ste izgubili napravo? [Izpis iz vseh mest](#)