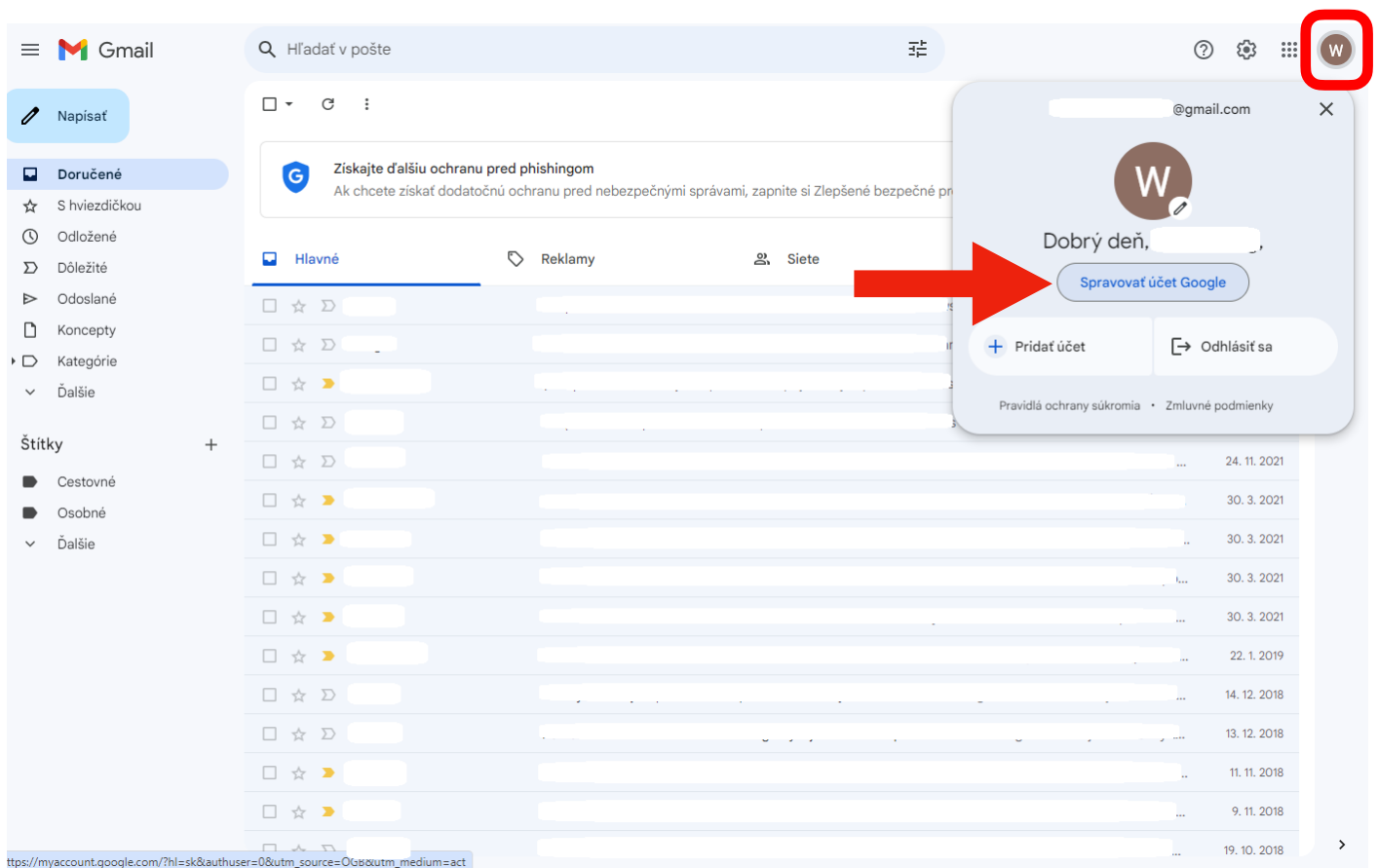


viacfaktorovú autentifikáciu

NA ÚČTE Google

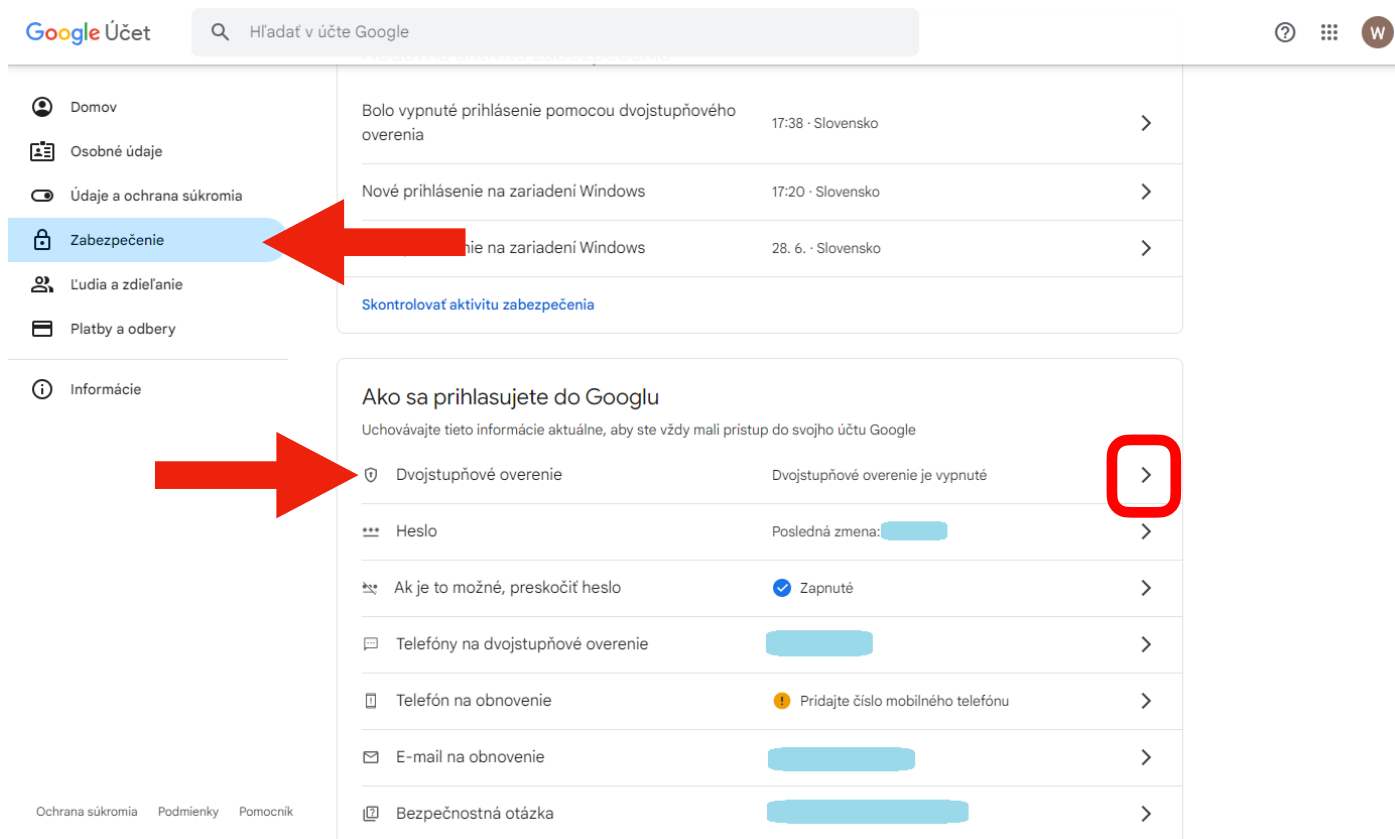
Vzhľadom na množstvo známych útokov na heslá používateľov a ich rastúcu sofistikovanosť nám už nepostačuje zabezpečenie našich účtov samotným heslom. Časté prípady kompromitovaných používateľských účtov, pracovných aj súkromných, a zverejňované databázy s miliónmi uniknutých prihlasovacích údajov nám dennodenne ukazujú potrebu lepšieho zabezpečenia nášho súkromia. Našťastie v dnešnej dobe už prevažná väčšina internetových služieb poskytuje možnosť okrem hesla zabezpečiť svoje účty ďalšími faktormi overovania používateľa. V tomto návode sa pozrieme, ako si jednoduchým spôsobom zabezpečiť pre únikom nášho hesla e-mailové konto od spoločnosti Google.

1) Prihláste sa do svojho účtu Google, resp. do vášho e-mailového konta na službe Gmail. Kliknite na vašu ikonu profilu. Zobrazí sa vám okno s možnosťou „Spravovať účet Google“. Kliknite na ňu.



Obr.1: Po kliknutí na ikonu používateľa vyskočí okno s možnosťou správy účtu Google.

2) Kliknite na záložku „Zabezpečenie“ na ľavej strane okna. Zobrazí sa vám menu, v ktorom si vyberte položku „Dvojstupňové overenie“. Kliknite na šípku v rovnakom riadku napravo.

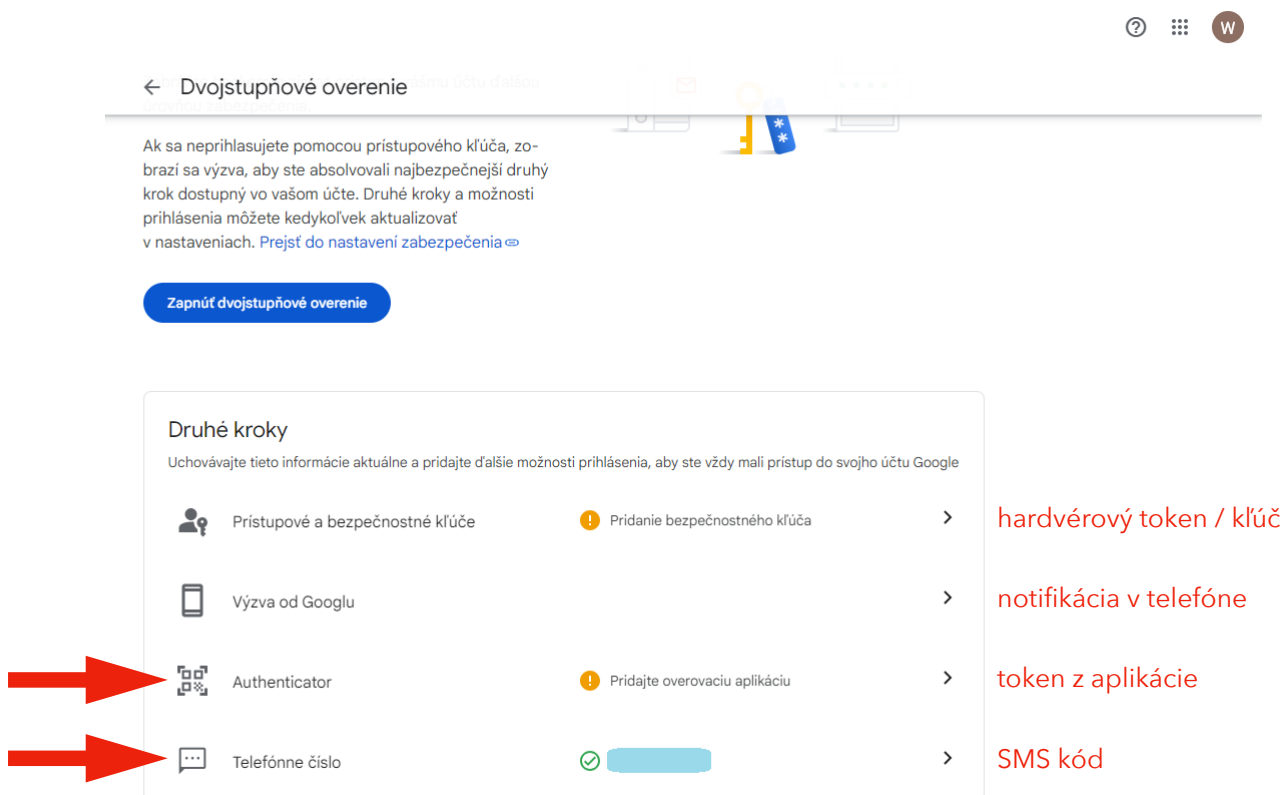


Obr.2: V záložke zabezpečenie sa nachádza voľba dvojstupňového overovania.

3) Ste v menu, ktoré ponúka na výber možnosti spôsobu overovania vášho prihlásenia. Môžete si zvoliť overovanie pomocou:

- bezpečnostných kľúčov, čo sú hardvérové kľúče alebo tokeny, podobné USB kľúčom,
- výzvy od Google, ktorá sa vám zobrazí na vašom telefóne ako notifikácia pri pokuse o prihlásenie po zadaní správneho hesla,
- autentifikátora, čo je aplikácia, ktorú si môžete stiahnuť do svojho telefónu a ktorá vám bude poskytovať jednorazové číselné kódy. Medzi najbežnejšie používané patria aplikácie **Microsoft Authenticator** a **Google Authenticator**,
- telefónneho čísla, kedy budete dostávať na svoj telefón SMS správy s jednorazovým číselným kódom.

V ďalšej časti návodu si predstavíme posledné dve možnosti.

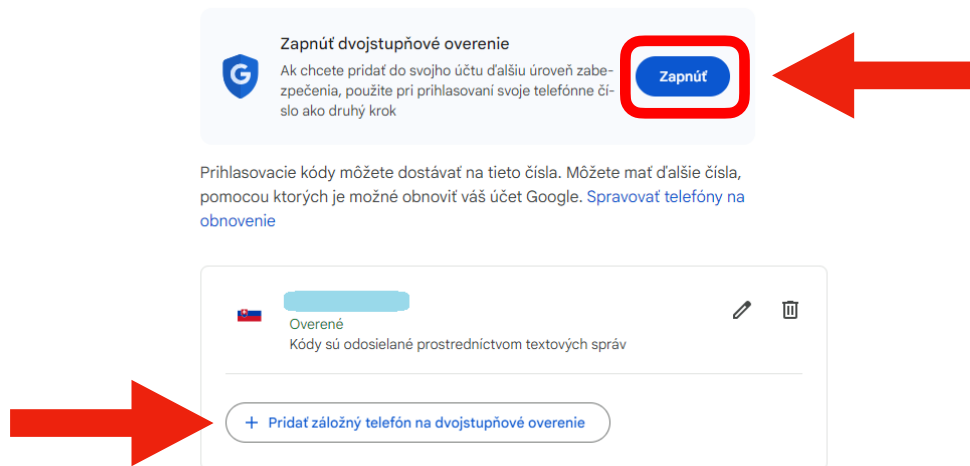


Obr.3: Menu s ponukou spôsobov overovania prihlásenia.

Autentifikácia pomocou SMS:

Kliknite na možnosť „Telefónne číslo“. Zobrazí sa vám menu s voľbou pridania telefónneho čísla pre váš účet. Pridajte číslo, na ktoré chcete dostávať SMS správu s jednorazovým autentifikačným kódom, ktorá vám príde vždy po úspešnom zadaní hesla pri prihlasovaní sa do vášho účtu Google. Kliknite následne „Zapnúť“ dvojstupňové overenie. Google si od vás v tomto kroku môže vyžiadať vaše heslo pre potvrdenie vašej totožnosti.

← Telefóny na dvojstupňové overenie

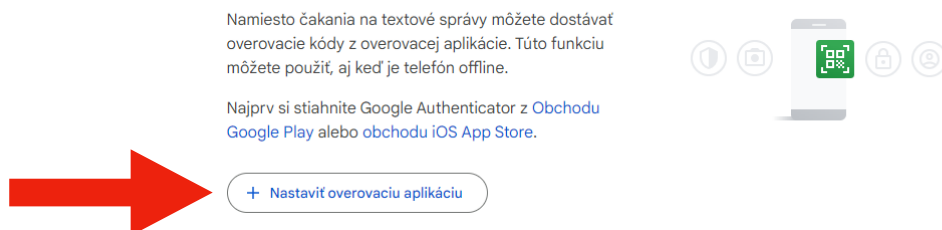


Obr. 4: Nastavenie MFA pomocou SMS.

Autentifikácia pomocou aplikácie:

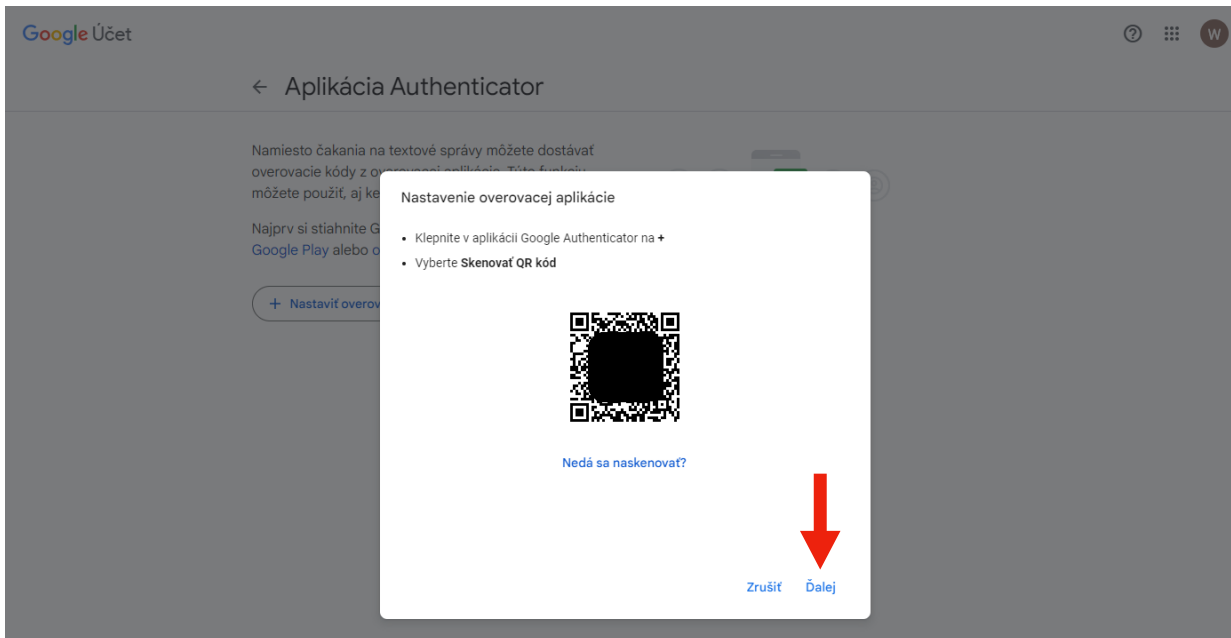
Kliknite na možnosť „Authenticator“. Pred začatím samotného procesu nastavenia tohto spôsobu overovania potrebujete mať v telefóne nainštalovanú autentifikačnú aplikáciu (napríklad **Google Authenticator**). Kliknite na voľbu „Nastaviť overovaciu aplikáciu“.

← Aplikácia Authenticator



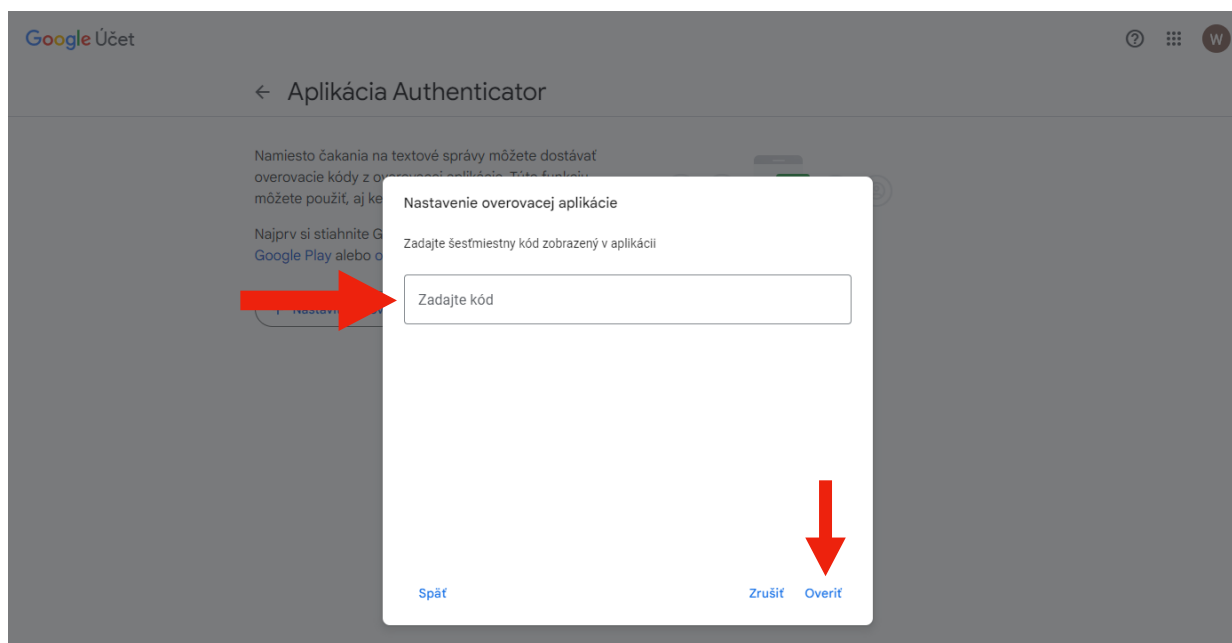
Obr.5: Začínáme s nastavením autentifikačnej aplikácie.

Google vám vygeneruje QR kód, ktorý stačí naskenovať do vašej autentifikačnej aplikácie. Tým si spárujete svoj účet Google s vašou aplikáciou. Kliknite na políčko „Ďalej“.



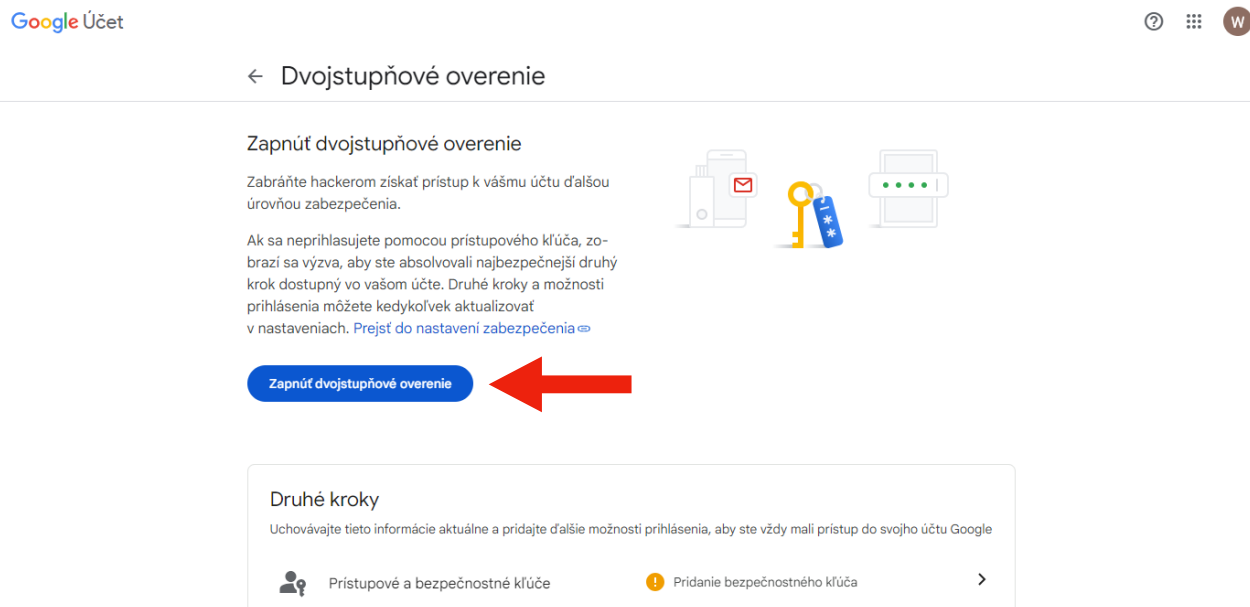
Obr.6: QR kód pre načítanie do aplikácie.

Aplikácia vám vygeneruje overovací kód, ktorý zadajte do políčka na to určeného. Kliknite „Overiť“.



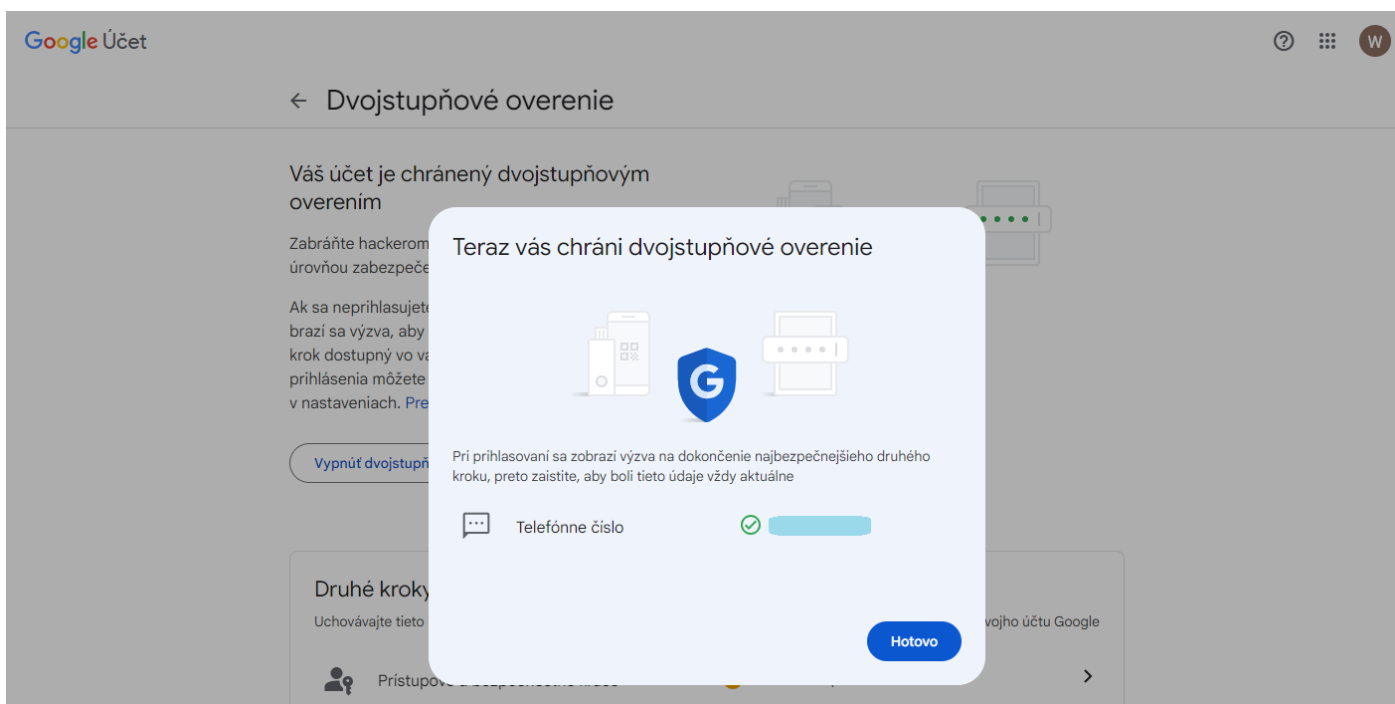
Obr.7: Pole pre vloženie overovacieho kódu z aplikácie.

Teraz už stačí len kliknúť na tlačidlo „Zapnúť dvojstupňové overovanie“ a nová funkcia v našom konte sa aktivuje.



Obr.8: Zapínáme dvojstupňové overovanie v účte Google.

Kliknite na „Hotovo“ a útočníci sa nedostanú do vášho účtu, aj keď by poznali vaše heslo.



Obr.9: Súhrnná informácia o aktivácii ďalšieho spôsobu overenia prihlásenia do vášho účtu.