Bitwarden Vaultwarden

Bitwarden je všestranný správce hesel s otevřeným zdrojovým kódem

- Bitwarden
- Dvoufázové přihlášení pro Twitter pomocí Vaultwarden
- Jak povolit dvoufaktorovou autentizaci na Mastodon

Bitwarden

Co je Bitwarden

Bitwarden je všestranný správce hesel s otevřeným zdrojovým kódem, který může být použit nejen jednotlivci k ukládání jejich kritických a důležitých informací, ale také jej mohou nasadit podniky na všech úrovních. Bitwarden lze stáhnout na mobilní telefony se systémem iOS i Android a poskytuje spoustu rozšíření prohlížeče pro automatické vyplňování hesel. Je to jeden z nejlepších open source správců hesel.

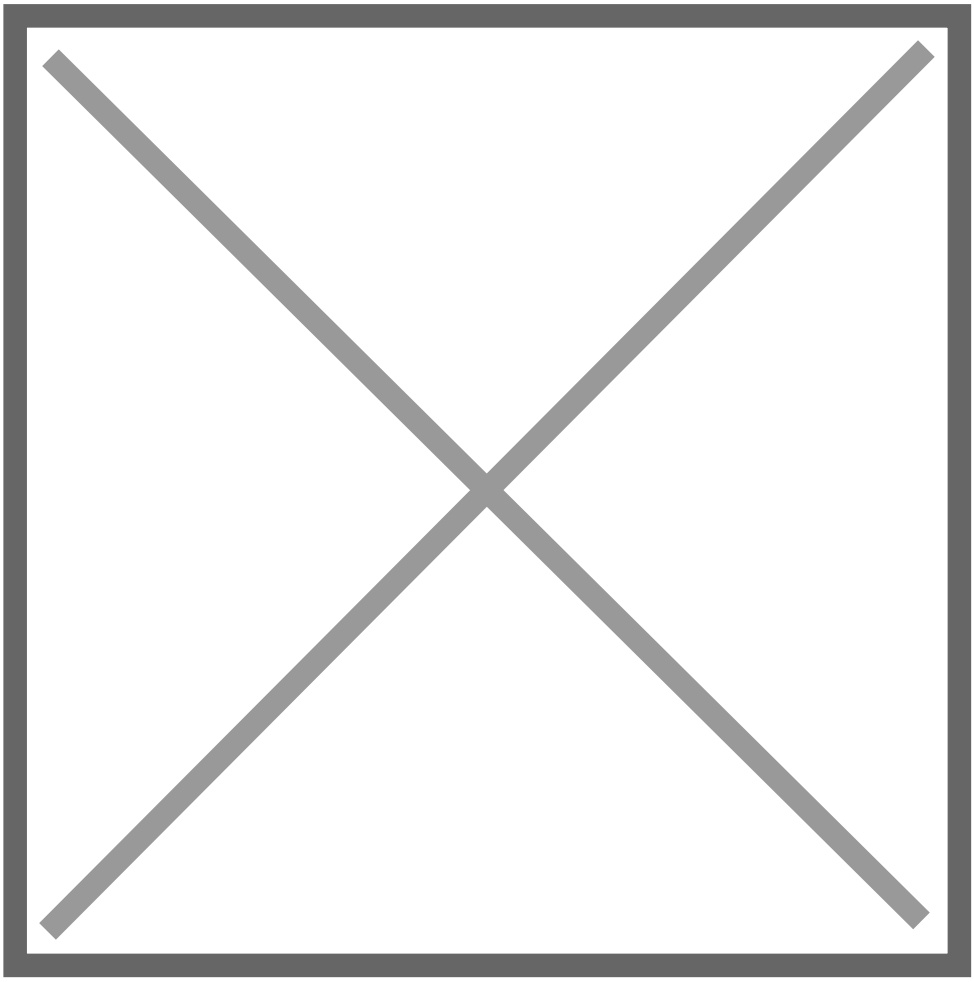
Nejen to, Bitwarden také poskytuje webové a desktopové aplikace spolu s rozhraním příkazového řádku, díky kterému je jedním z nejlepších multiplatformních správců hesel, které pokrývají všechny klientské aplikace. Můžete jej snadno použít jako desktopovou aplikaci pro macOS, Linux a Windows.

Pokud jde o ochranu informací uložených na Bitwarden, správce hesel používá 256bitový šifrovací protokol AES, který znemožňuje hackování a vloupání. Kromě toho jsou všechny informace uloženy v zašifrovaném trezoru, ke kterému má vlastník přístup pouze prostřednictvím hlavního klíče.

Vytvořte si účet Bitwarden

Na námi hostovaný Bitwarden se můžete registrovat zde

Na obrazovce Vytvořit účet vyplňte všechna pole (Nápověda k hlavnímu heslu je volitelná) a vyberte **Odeslat** .

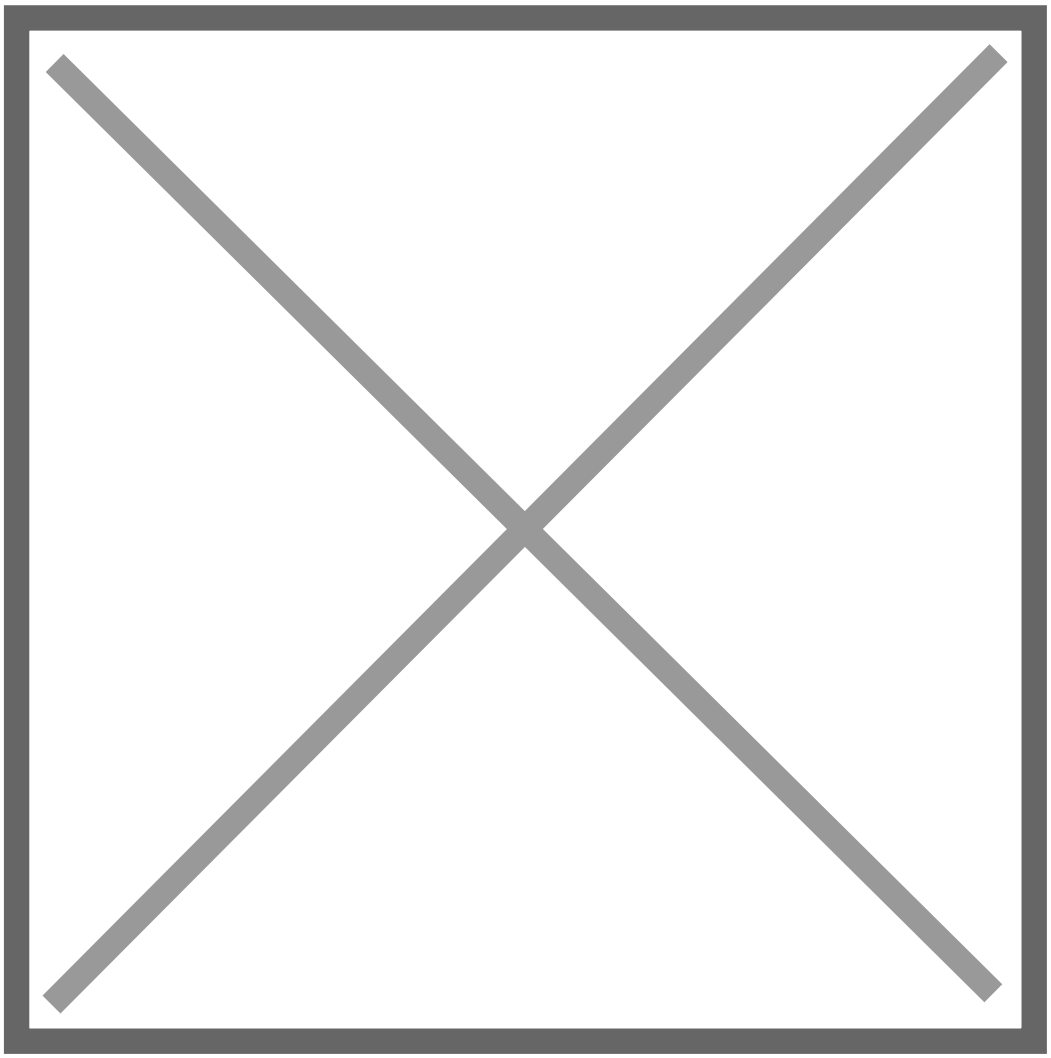


Vytvořte si účet

Jakmile si vytvoříte svůj účet, požádejte Bitwarden, aby vám poslal ověřovací e-mail tak, že se přihlásíte do svého webového trezoru a vyberete tlačítko **Ověřit e-mail** .

Začněte s Web Vault

Webový trezor Bitwarden poskytuje osobním uživatelům a organizacím nejbohatší prostředí Bitwarden. Mnoho důležitých funkcí, jako je nastavení dvoufázového přihlášení nebo správa organizace , musí být prováděno z webového trezoru.



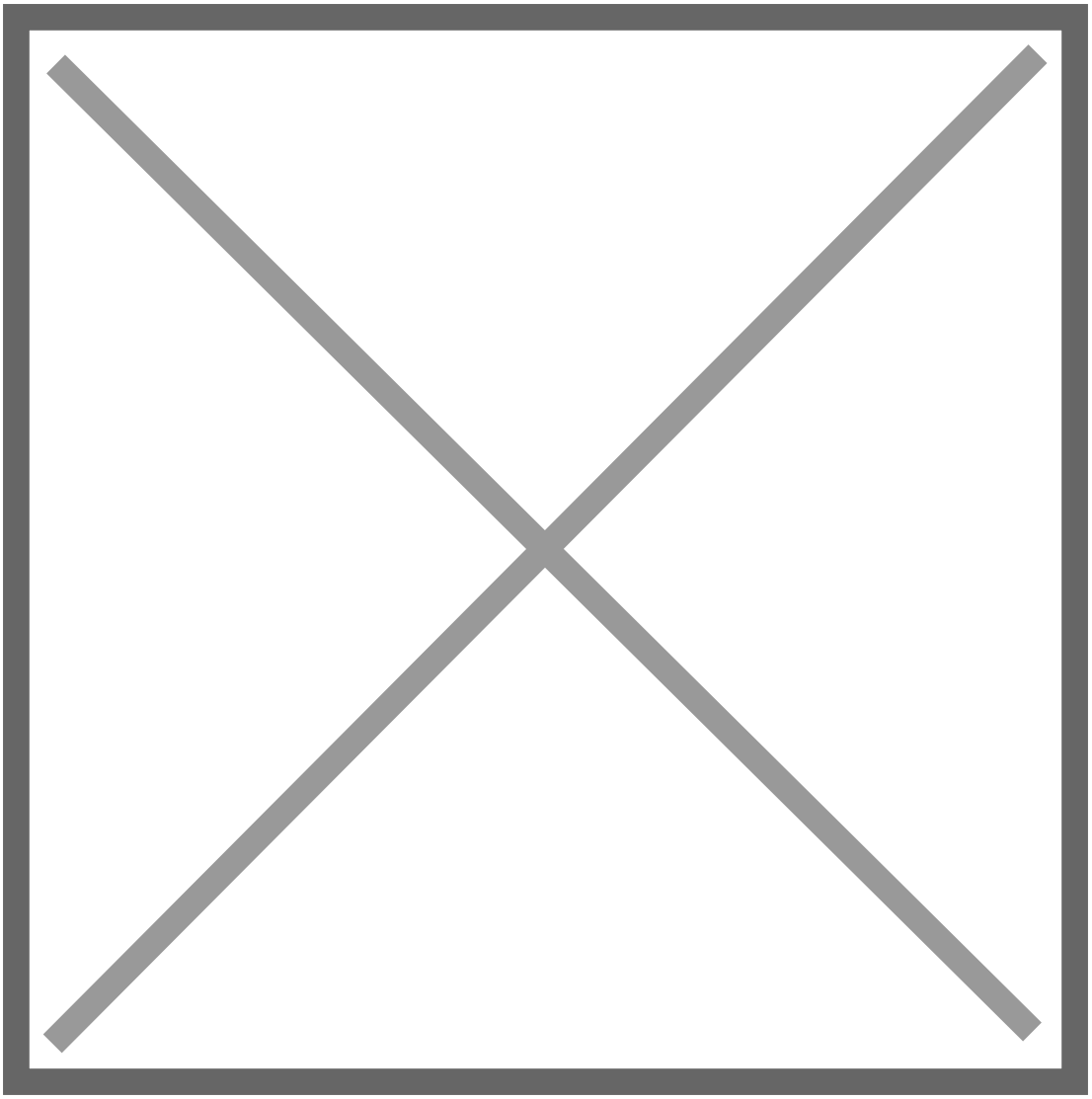
Když se poprvé přihlásíte do svého webového trezoru, dostanete se do **zobrazení Trezoru**. V tomto prostoru budou uvedeny všechny položky trezoru, včetně přihlašovacích údajů, karet, identit a bezpečnostních poznámek .

Na předchozím snímku obrazovky se v **zobrazení Trezor**u zobrazuje **Všechny položky** v **mém trezoru** . Uživatelé organizací zde budou mít uvedeny další trezory. Pomocí **sloupce Filtry** můžete uspořádat úschovnu do **Oblíbených** a **Složek** .

Začněme nastavením nové složky a přidáním nového přihlašovacího jména:

Chcete-li vytvořit složku:

- Vyberte ikonu **Přidat** vedle části Složky ve sloupci Filtry.
- Zadejte název (např. `Sociální sítě`) pro vaši složku a vyberte **Uložit** .



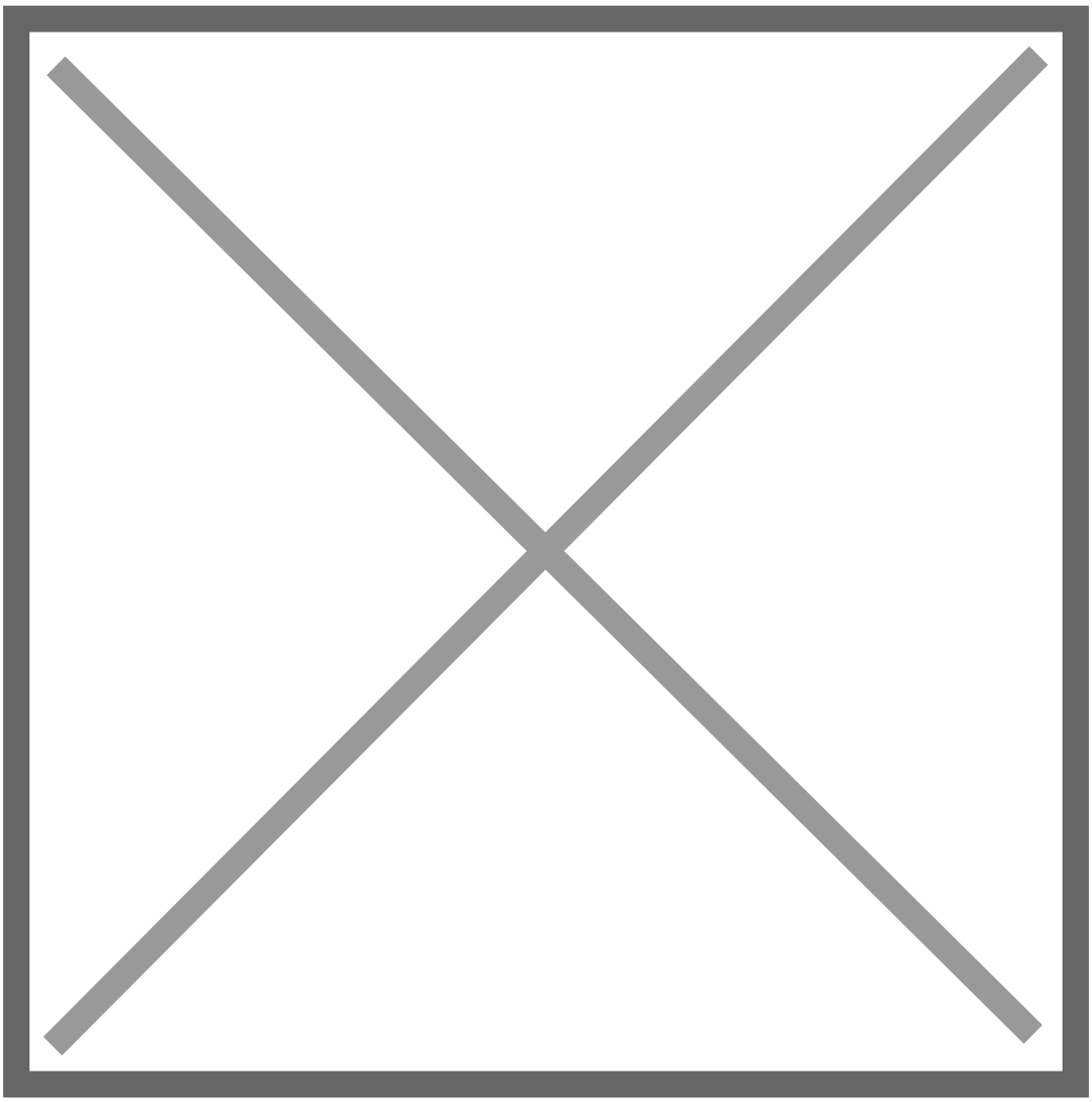
Vytvoření složky

Přidejte položku přihlášení

Chcete-li přidat novou položku přihlášení:

1. Vyberte tlačítko **Přidat položku** .
2. Z rozevírací nabídky vyberte možnost **Přihlásit** (pokud místo toho přidáváte kartu, identitu nebo zabezpečenou poznámku, vyberte tuto možnost).
3. Zadejte **název** položky. Názvy vám pomohou snadno identifikovat položky ve vašem trezoru, proto dejte této položce rozpoznatelnou (např. `Mastodon Arch Linux`).
4. Zadejte své **uživatelské jméno** a **heslo** . Prozatím zadejte své stávající heslo. vám jej pomůžeme nahradit silnějším heslem později.
5. Do pole **URI 1** zadejte adresu URL webové stránky (např. `https://mastodon.arch-linux.cz`). Pokud nevíte, jakou adresu URL použít, přejděte na přihlašovací obrazovku webové stránky a zkopírujte ji z adresního řádku.
6. Z rozevíracího seznamu **Složka** vyberte název složky, do které chcete přidat tuto položku (např `Sociální sítě` složku, kterou jsme vytvořili dříve). Chcete -li tuto položku přidat mezi

oblíbené, vyberte ikonu hvezdičky.
7. Klepnutím na **tlačítko Uložit** dokončíte přidávání této položky.



Přidání položky

Vygenerujte si silné heslo

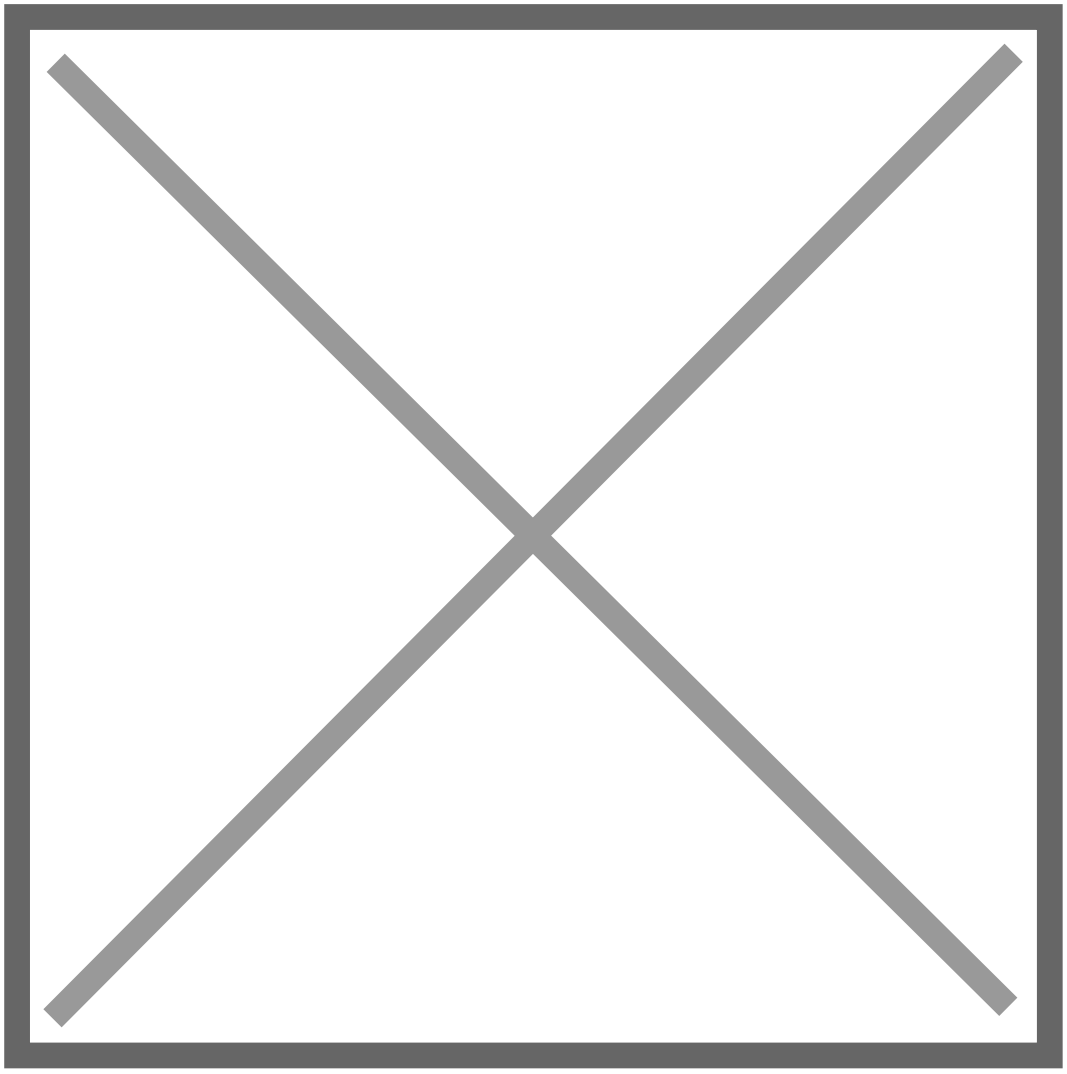
Nyní, když je ve vašem trezoru uloženo nové přihlášení, vylepšete jeho zabezpečení nahrazením stávajícího hesla silnějším:

1. Ve svém trezoru vyberte položku, kterou chcete zabezpečit.
2. Na nové kartě nebo okně otevřete odpovídající webovou stránku a přihlaste se ke svému účtu.
3. Na tomto webu přejděte do oblasti, kde můžete **změnit heslo** . Obvykle to najdete v **části Váš účet** , **Zabezpečení** , **Nastavení** přihlášení nebo **Nastavení přihlášení** .
4. Většina webových stránek vyžaduje nejprve zadání **aktuálního hesla** . Vraťte se do svého trezoru a vyberte ikonu **Kopírovat** vedle **pole Heslo** . Poté se vraťte na web a vložte jej do pole **Aktuální heslo** . Možná si staré heslo zapamatujete, ale je dobré si

zvyknout heslo zkopírovat a vložit. Takto se budete přihlašovat, jakmile bude vaše heslo nahrazeno silnějším.

5. Vraťte se do svého trezoru a klikněte na ikonu **Generovat** vedle **pole Heslo** . Budete dotázáni, zda chcete přepsat aktuální heslo, takže **výběrem Ano .** pokračujte Toto nahradí vaše **heslo** náhodně vygenerovaným silným heslem. Přesun z hesla jako `1234` na `x*wNvUpKagnv^5q9m74X` může zastavit hackera.
6. Zkopírujte své nové heslo pomocí stejné ikony **Kopírovat** , kterou jste použili dříve, a vyberte tlačítko **Uložit** .
7. Vraťte se na druhý web a vložte své silné heslo do **Nové heslo** a **Potvrdit nové heslo .**
8. Jakmile **uložíte** změnu hesla, máte nové heslo hotovo!

tip: Nedělejte si starosti s přepsáním svého stávajícího hesla! Pokud se něco pokazí, Bitwarden udržuje **historii hesel** posledních pěti hesel pro každé přihlášení: View Password History



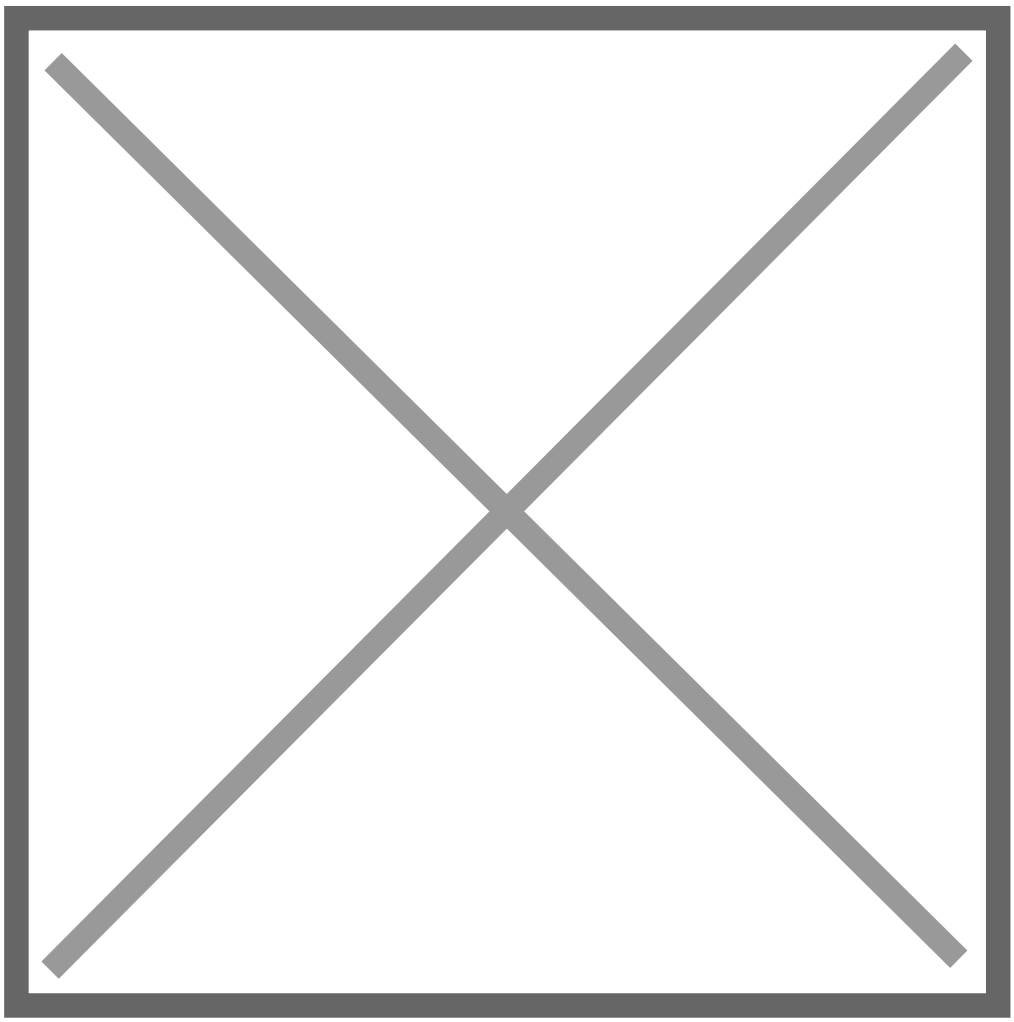
Historie hesel

Zabezpečte svůj trezor

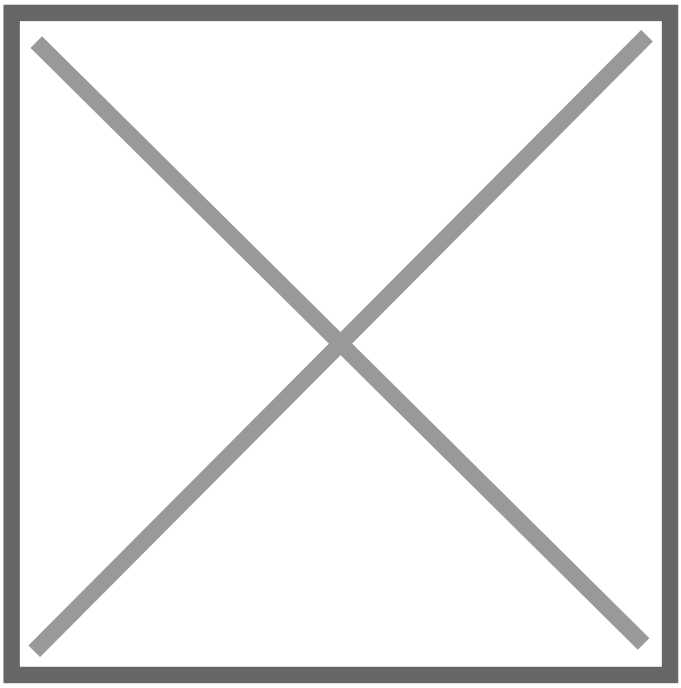
Nyní, když je váš trezor plný dat, pojďme podniknout kroky k jeho ochraně nastavením dvoufázového přihlášení. Dvoufázové přihlášení vyžaduje, abyste při přihlašování ověřili svou identitu pomocí dalšího tokenu, který je obvykle načten z jiného zařízení.

Existuje mnoho dostupných metod pro dvoufázové přihlášení, ale doporučenou metodou pro bezplatný účet Bitwarden je použití aplikace pro ověřování mobilních zařízení, jako je Authy :

1. Stáhněte si Authy do svého mobilního zařízení.
2. Ve svém webovém trezoru vyberte ikonu profilu a **účtu : vyberte Nastavení** z rozbalovací nabídky



1. Z **nabídky Nastavení účtu** vyberte stránku **Zabezpečení** a **kartu Dvoufázové přihlášení**
2. Vyhledejte možnost **Authenticator App** a vyberte **Spravovat** :
   Manage Authenticator App Správa aplikace Authenticator Budete vyzváni k zadání hlavního hesla, abyste mohli pokračovat
3. Na mobilním zařízení otevřete Authy a klepněte na tlačítko **Přidat účet** .



4. Naskenujte QR kód umístěný ve vašem webovém trezoru pomocí Authy. Po naskenování Authy zobrazí šestimístný ověřovací kód.
5. Zadejte šestimístný ověřovací kód do dialogového okna ve vašem webovém trezoru a vyberte tlačítko **Povolit** .
6. Klepnutím na **tlačítko Zavřít** se vraťte na obrazovku dvoufázového přihlášení a vyberte tlačítko **Zobrazit kód obnovení** . Váš obnovovací kód lze použít v případě, že ztratíte své mobilní zařízení. **Toto je kritický krok, který zajistí, že se nikdy nedostanete do svého trezoru** , takže ho nepřeskakujte!
7. Zadejte své hlavní heslo a kliknutím na **tlačítko Pokračovat** získejte kód pro obnovení. Example Recovery Code Př

Uložte si kód pro obnovení způsobem, který vám dává největší smysl. Věřte tomu nebo ne, vytištění kódu pro obnovení a jeho uložení na bezpečném místě je jedním z nejlepších způsobů, jak zajistit, aby kód nebyl zranitelný vůči krádeži nebo nechtěnému smazání.

Dvoufázové přihlášení pro Twitter pomocí Vaultwarden

Tento návod vás provede nastavením dvoufázového přihlášení pro váš účet Twitter pomocí Vaultwarden a vestavěného Vaultwarden Authenticator.

Přejděte na web Twitter

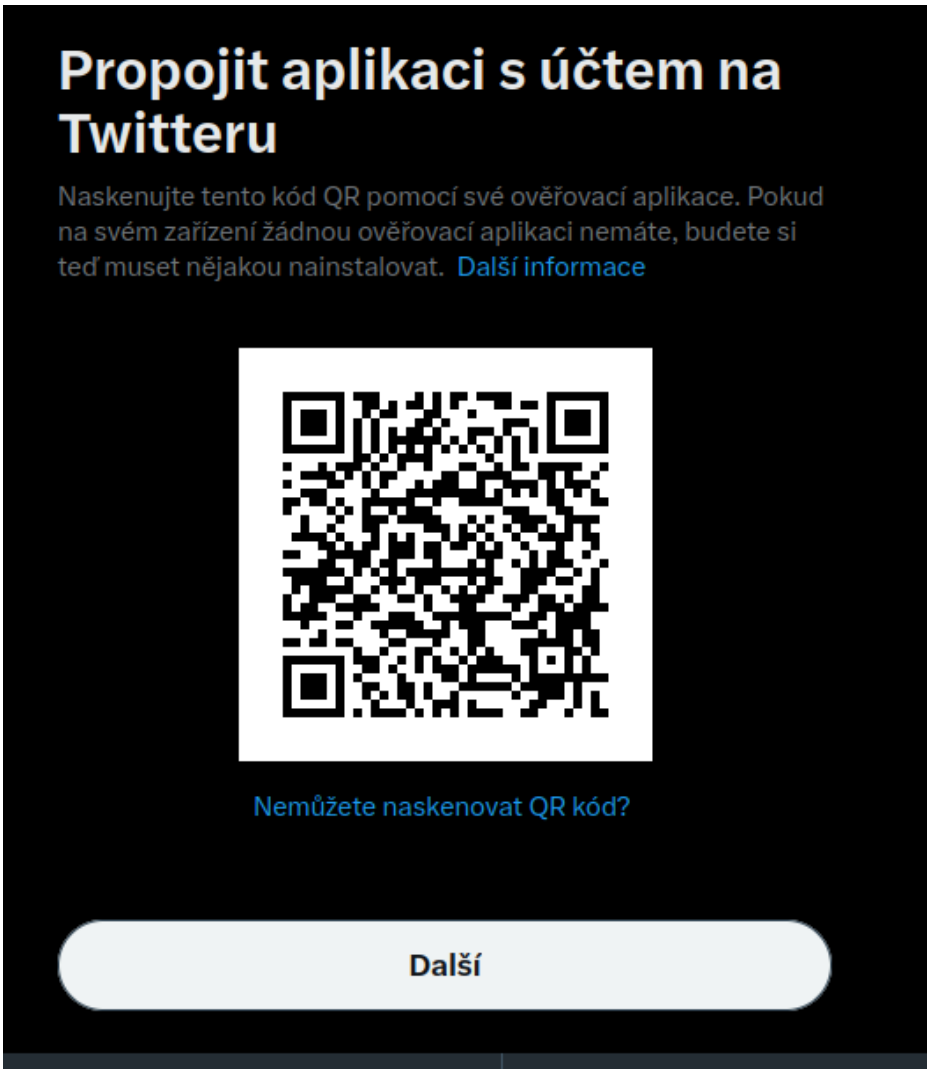
Na webu Twitteru vyberte možnosti nabídky se třemi tečkami „Další“ na levé straně. Odtud vyberte „Nastavení a soukromí“ a poté „Zabezpečení“ a poté „Dvoufaktorové ověření“.

Twitter nabízí tři možnosti ověření: textovou zprávu, bezpečnostní klíč a ověřovací aplikaci Textová zpráva je možná nejméně bezpečnou možností, protože jsou známé scénáře, kdy mohou útočníci přenést vaše telefonní číslo na novou SIM kartu bez vašeho vědomí. To se nazývá SIM jacking. K dispozici je také možnost hardwarového bezpečnostního klíče, což je dobrá volba.

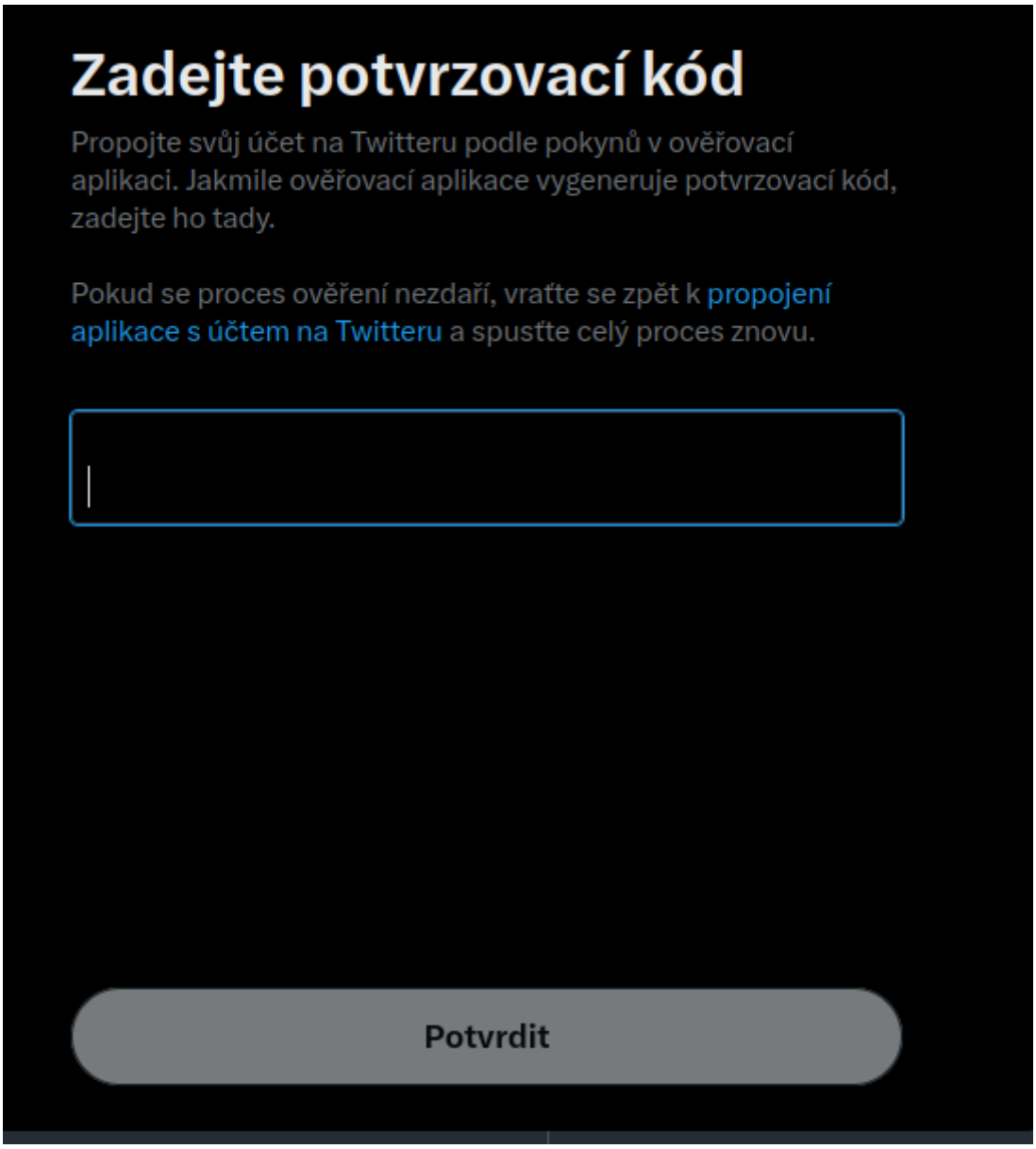
Zvolili bychom dvoufázové přihlášení pomocí aplikace Authenticator a zde vstupuje do hry náš Vaultwarden.

Zachyťte ověřovací kód

Nakonec budete vyzváni pomocí QR kódu ke skenování pomocí aplikace Authenticator. Zde můžeme použít autentizátor Vaultwarden, který je součástí funkcí našeho Vaultwarden



Uložte záznam a poté získáte 6místný token z vaší aplikace pro vstup na web Twitter.



Vygenerujte a uložte záložní kódy

Podobně jako když nastavujete dvoufázové přihlášení na jakékoli webové stránce, často vám budou poskytnuty záložní kódy, pokud byste někdy ztratili svou původní autentizační schopnost. Sledování záložních kódů je důležité! Je VELMI DŮLEŽITÉ, abyste vygenerovali a uložili záložní kódy na bezpečném místě, odděleně od vašich dalších přihlašovacích údajů na Twitteru. Můžete dokonce chtít vygenerovat několik kódů v textovém souboru (bez ukládání) a poté jej vytisknout pro bezpečné uchování.

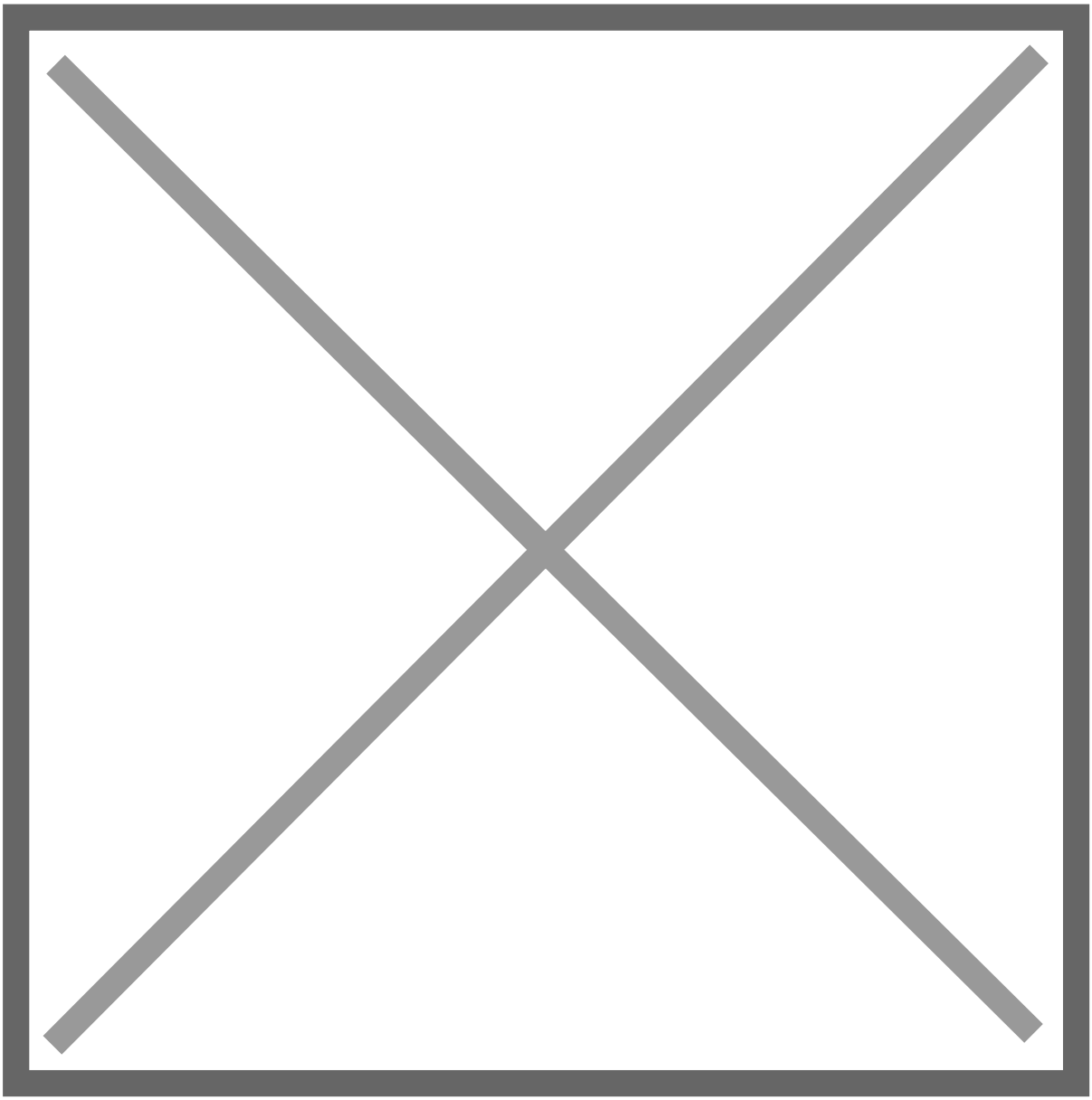
Jak povolit dvoufaktorovou autentizaci na Mastodon

Jak povolit dvoufaktorové ověření na Mastodon

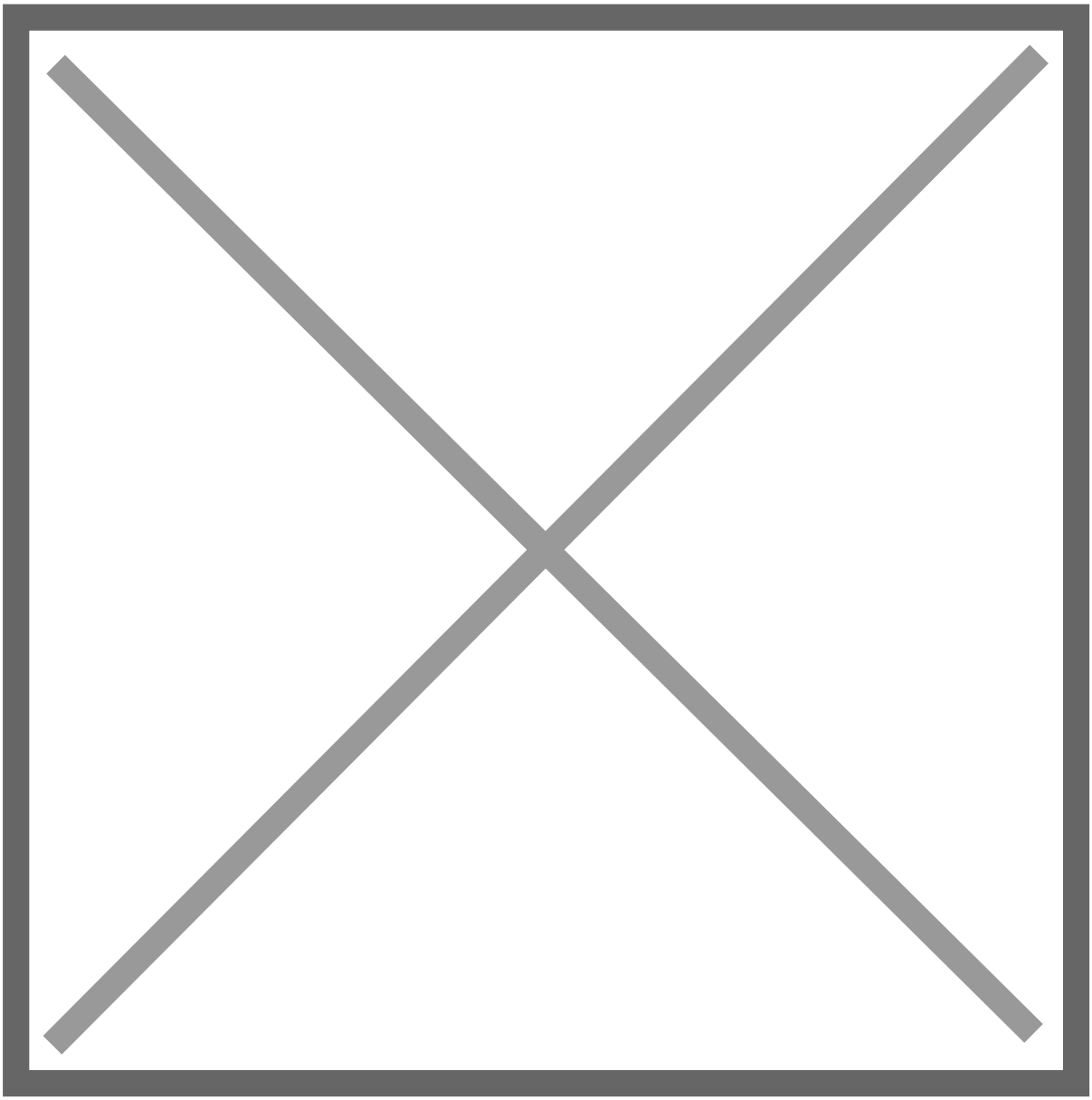
Dvoufaktorové ověření nabízí přidaný stupeň ochrany přístupu k vašemu Mastodon účtu. Kromě samotného hesla k účtu je při přístupu vyžadován také ověřovací klíč, který je zasílán na Vaše mobilní zařízení. Dvoufaktorové ověření zabraňuje neoprávněným uživatelům a zařízením v přístupu k vašemu účtu. Pro dvoufaktorové ověření můžete začít používat, správce hesel naší komunity Vaultwarden postaveném na Bitwardenu.

Chcete-li povolit 2FA na Mastodon, oficiální metoda je:

Nastavení > Nastavení účtu > Dvoufaktorové ověření > Nastavit



Nyní vám bude nabídnut QR kód, který můžete naskenovat pomocí aplikace Google Authenticator nebo třeba pomocí u nás spravovaného správce hesel Vaultwarden



Nyní stačí v aplikaci Vaultwarden stisknout tlačítko Autentizační klíč (TOTP) a naskenovat QR kód, uložte. Teď opište ověřovací kód do kolonky **Kód pro dvoufázové ověření *** a již jen **zapnout**

Nyní máte dvoufázové ověřování zapnuté. Ztratíte-li někdy přístup ke svému telefonu, můžete k získání přístupu k účtu použít jeden ze záložních kódů. **Uchovejte tyto kódy v bezpečí**..