



## Bezpečnější přihlašování k poště a službám Microsoft 365

### Konfigurace autentizačního tokenu

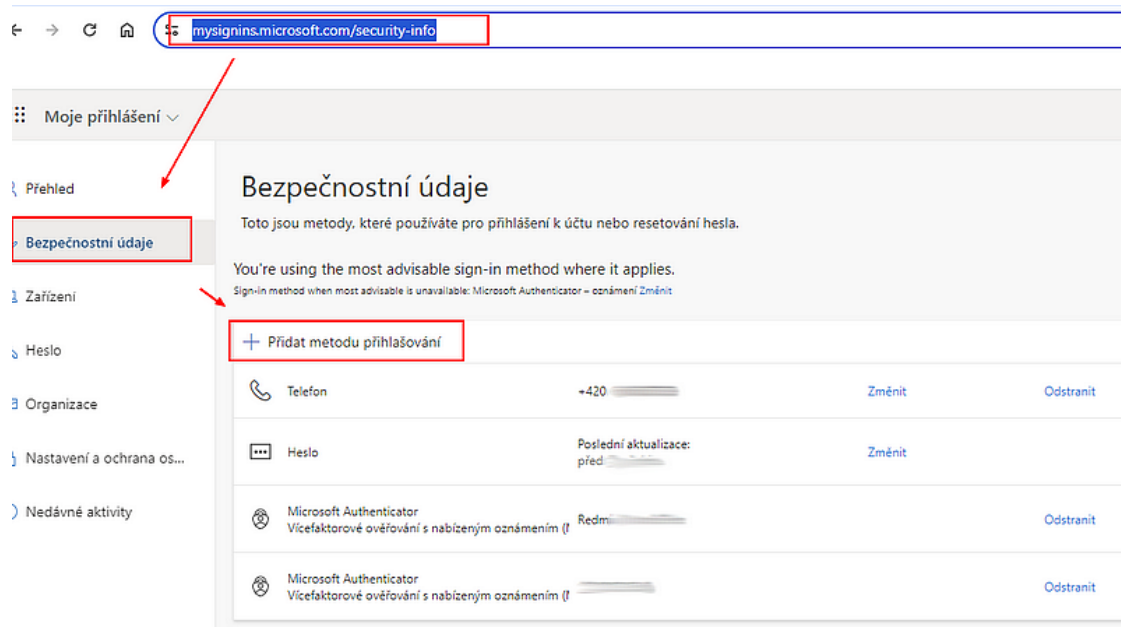
Využijte možnosti lépe zabezpečit svůj účet a poštovní schránku před zneužitím přihlašovacích údajů prostřednictvím **multifaktorové autentizace (MFA)** v Microsoft 365. Jedná se o klíčový nástroj pro zvýšení bezpečnosti vašich dat a informací.

### Zde jsou hlavní důvody, proč byste měli začít využívat MFA:

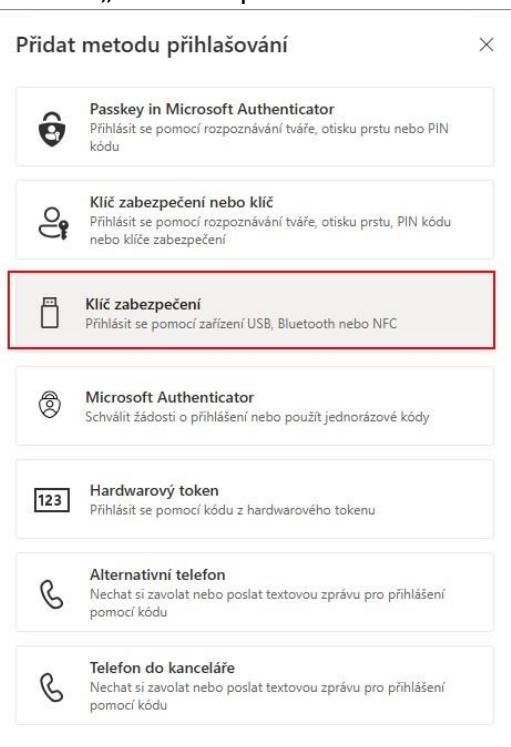
1. **Zvýšená bezpečnost:** MFA výrazně snižuje riziko úniku dat tím, že vyžaduje více než jednu formu ověření. To znamená, že i když je heslo kompromitováno, útočník stále nebude moci získat přístup k účtu.
2. **Flexibilita:** MFA v Microsoft 365 v současné době nabízí různé metody ověření, včetně textových zpráv, mobilních aplikací a autentizačních tokenů. To umožňuje uživatelům vybrat si metodu, která je pro ně nejpohodlnější.
3. **Snadná implementace:** MFA je snadno implementovatelná a nevyžaduje žádné speciální technické dovednosti. Pokud by se přece jen něco nepodařilo, jsou vám připraveni pomoci pracovníci Centra služeb, případně správci z oddělení informačních technologií.
4. **Kompatibilita:** MFA je kompatibilní s většinou zařízení a platforem, včetně mobilních telefonů, tabletů a počítačů.

## Jak si mám multifaktorovou autentizaci aktivovat?

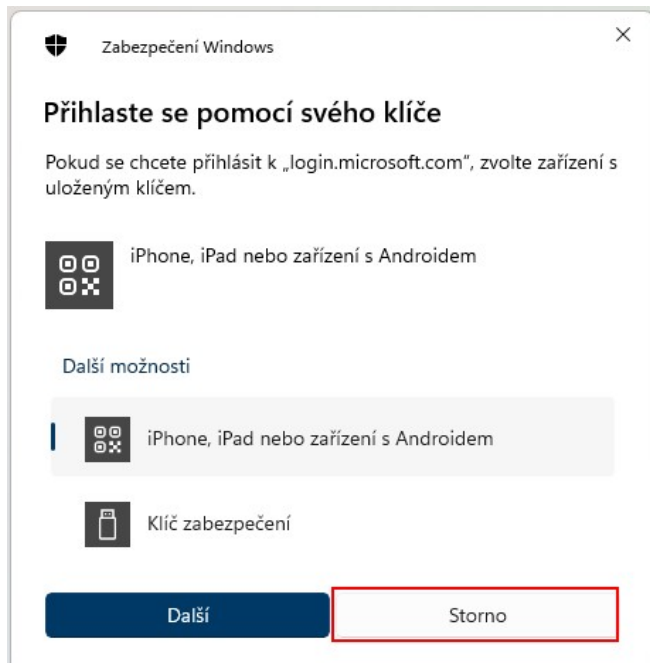
1. Na webové stránce <https://mysignins.microsoft.com/security-info> jsou na výběr různé metody zabezpečení, můžete si jich vybrat i vícero. Seznam metod je k dispozici pod položkou „Přidat metodu ověřování“



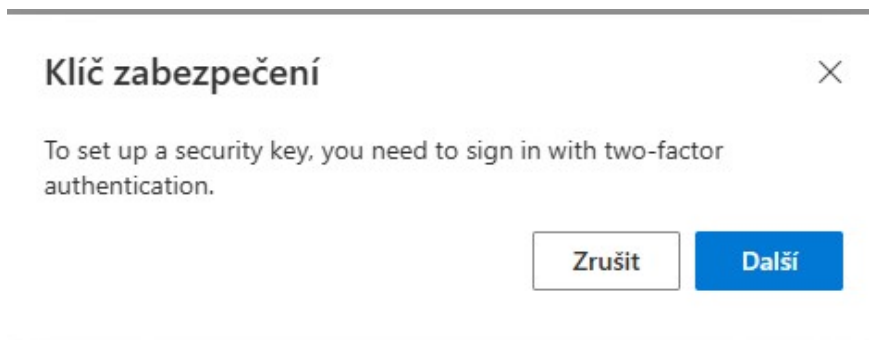
2. Primárně doporučujeme nastavit mobilní aplikaci **Microsoft Authenticator**. Další možností pro vícefaktorové ověřování je použít autentizační token. Vyberte metodu „Klíč zabezpečení“.



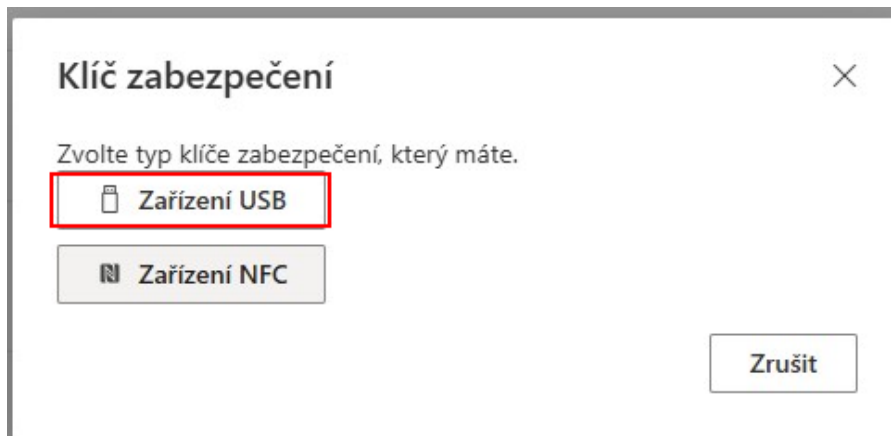
3. V případě, že máte již registrovaný jiný autentizační klíč nebo jinou metodu vícefaktorové autentizace, může se vám zobrazit následující dialog.



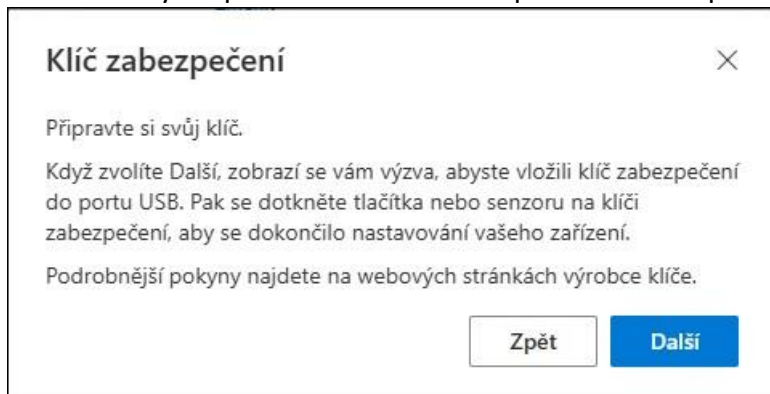
Pro použití Microsoft Authenticatoru nebo textové zprávy zvolte „Další“.



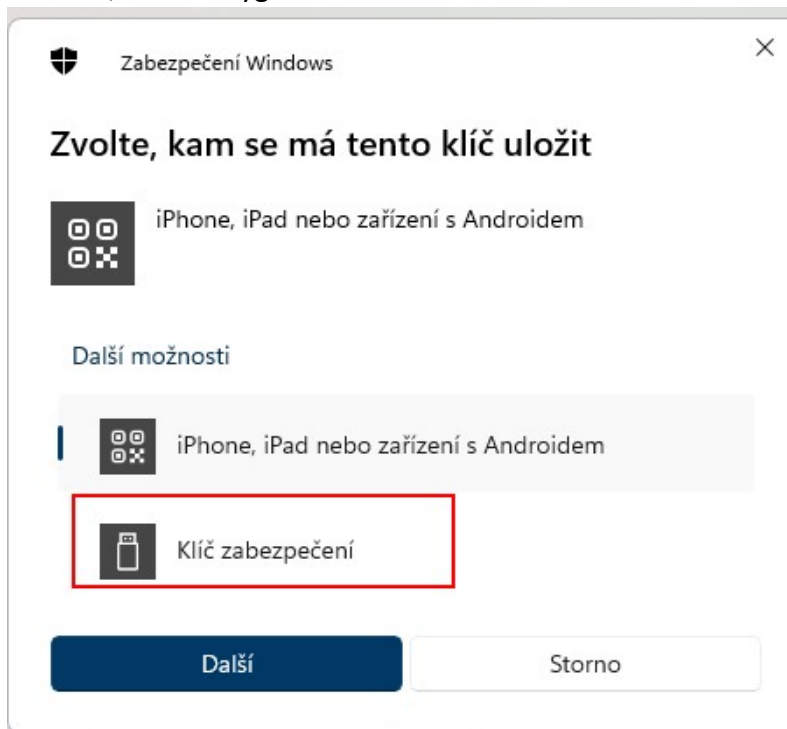
4. Následně je třeba zvolit typ klíče, který používáte. V tomto případě zvolíme zařízení USB.



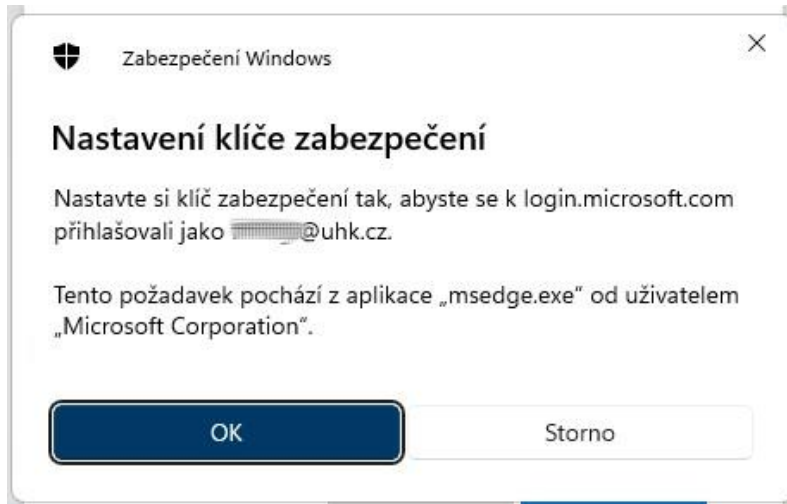
5. Zobrazí se výzva pro vložení klíče zabezpečení do USB portu



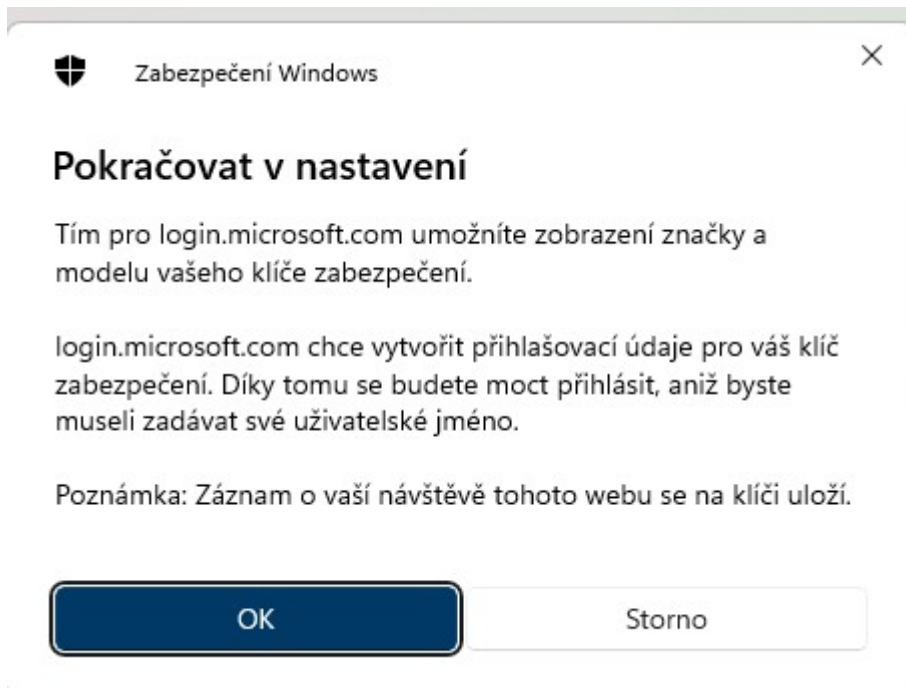
6. Zvolíme, uložení vygenerovaného klíče na autentizační token



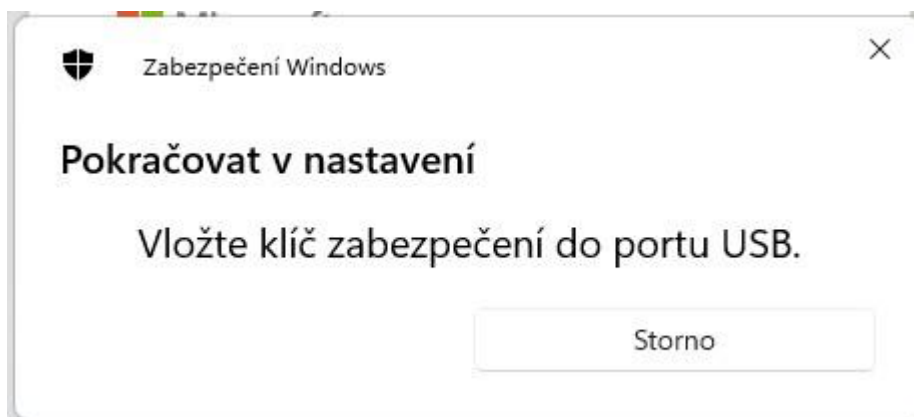
7. Zkontrolujeme, že uvedené údaje souhlasí.



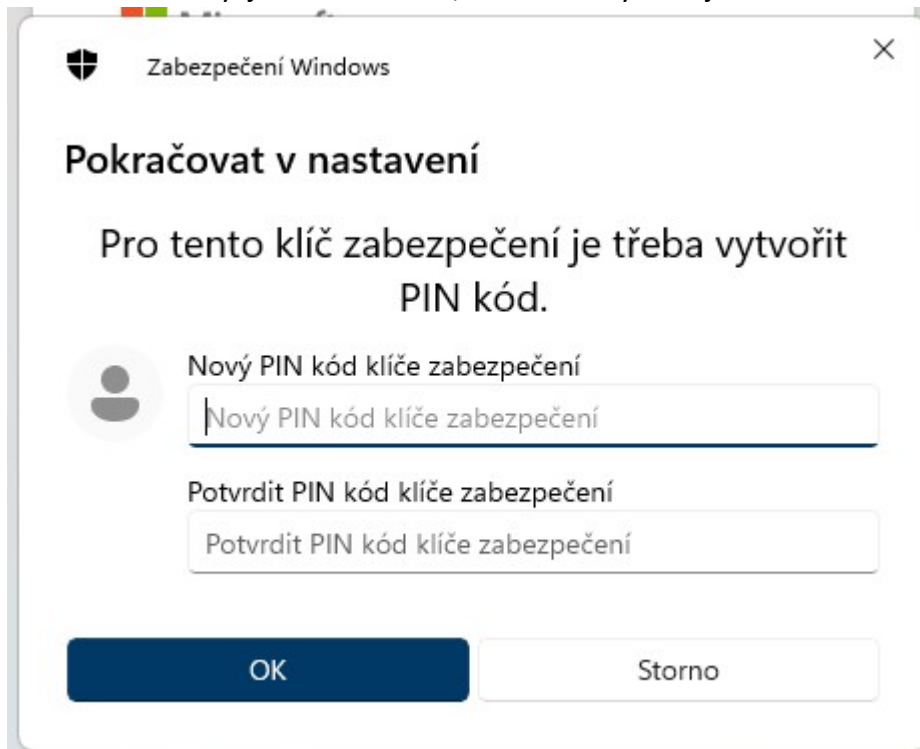
8. Potvrdíme další krok nastavení



9. Vložíme autentizační token do zařízení, kde provádíme nastavení.

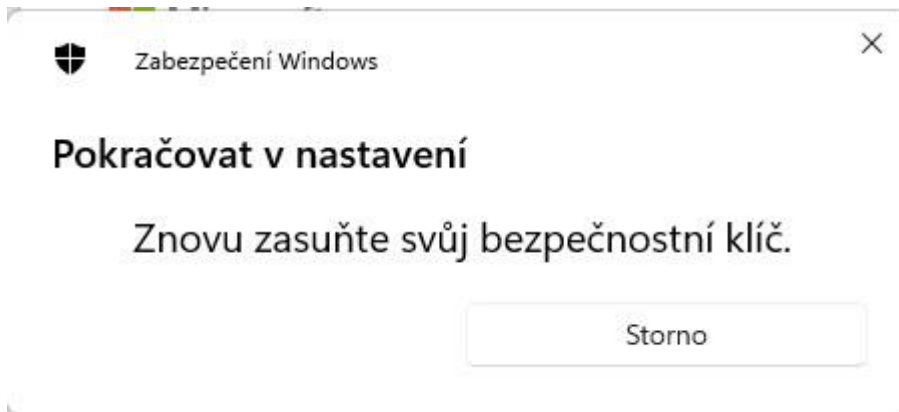


10. Pokud se jedná o nový token, zobrazí se výzva pro zadání PINu k autentizačnímu tokenu. Pokud byl již PIN nastaven, zobrazí se výzva k jeho zadání.



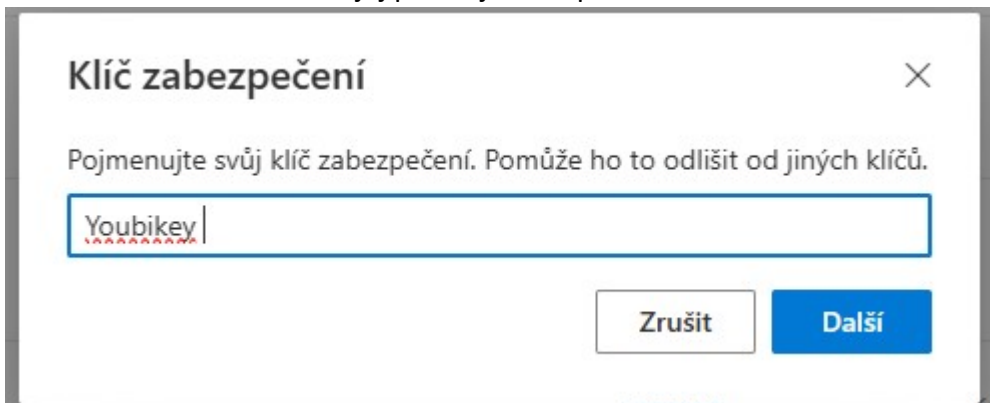
The screenshot shows a Windows Security dialog box titled "Zabezpečení Windows". The main heading is "Pokračovat v nastavení". Below it, the text reads "Pro tento klíč zabezpečení je třeba vytvořit PIN kód." There are two input fields: "Nový PIN kód klíče zabezpečení" and "Potvrdit PIN kód klíče zabezpečení". At the bottom, there are two buttons: "OK" and "Storno".

11. Zobrazí se výzva k vyjmutí a opětovnému vložení klíče do USB portu.

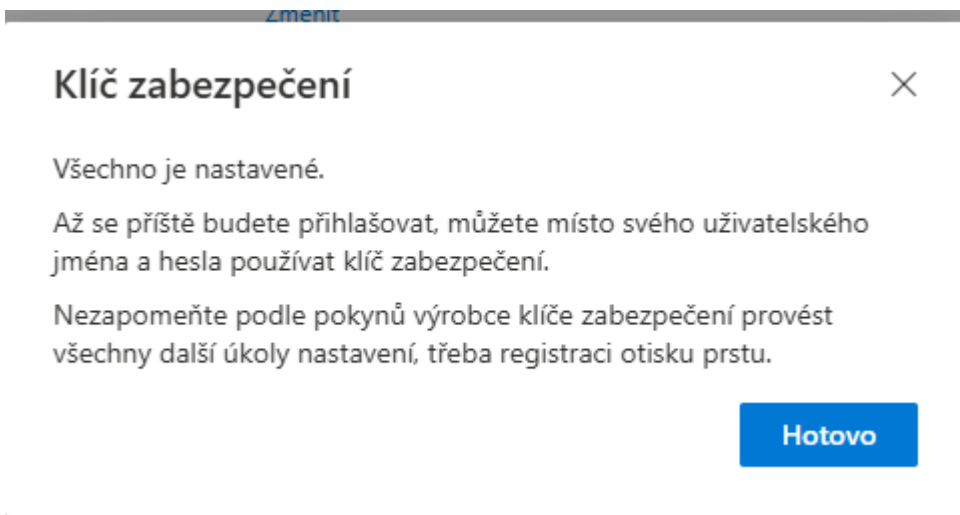


The screenshot shows a Windows Security dialog box titled "Zabezpečení Windows". The main heading is "Pokračovat v nastavení". Below it, the text reads "Znovu zasuňte svůj bezpečnostní klíč." At the bottom, there is a single button labeled "Storno".

12. Pokud vše proběhlo v pořádku, zobrazí se výzva k pojmenování autentizačního tokenu. Pod tímto názvem jej pak najdete v portálu M365



13. Přidání tokenu proběhlo úspěšně. Pokračujte dalším krokem k aktivaci vícefaktorové autentizace.

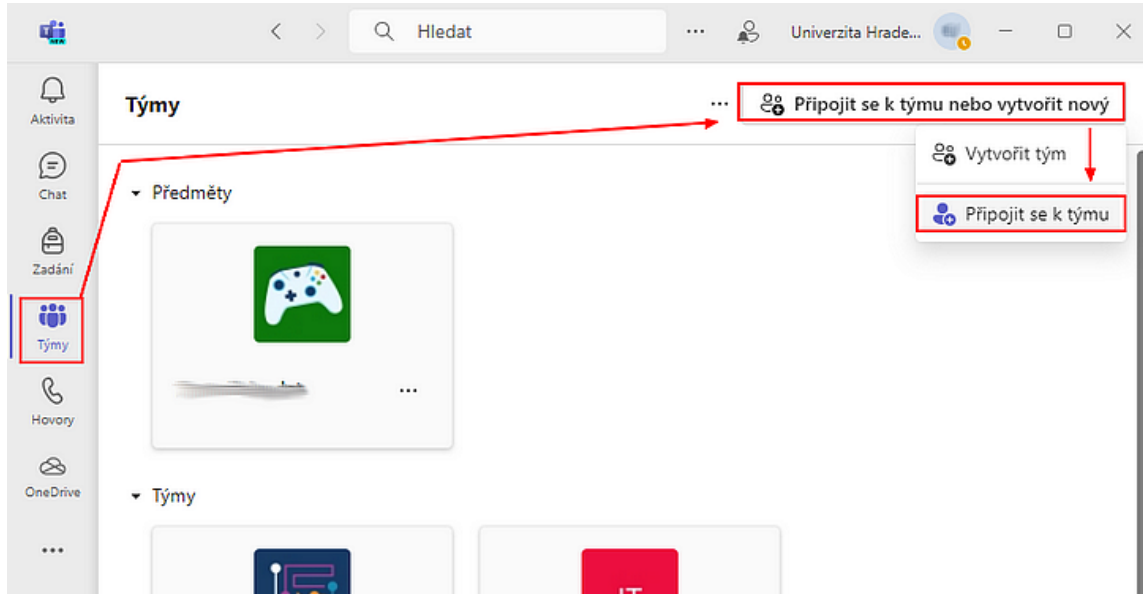


14. Pokud se tak již nestalo, přidejte si pro jistotu záložní formu ověřování na webové stránce uvedené v kroku 1. Lze použít například sms ověřování. Můžete si také nainstalovat Microsoft Authenticator i na další zařízení, například tablet. Postupujte vždy dle instrukcí ve webovém portálu M365.

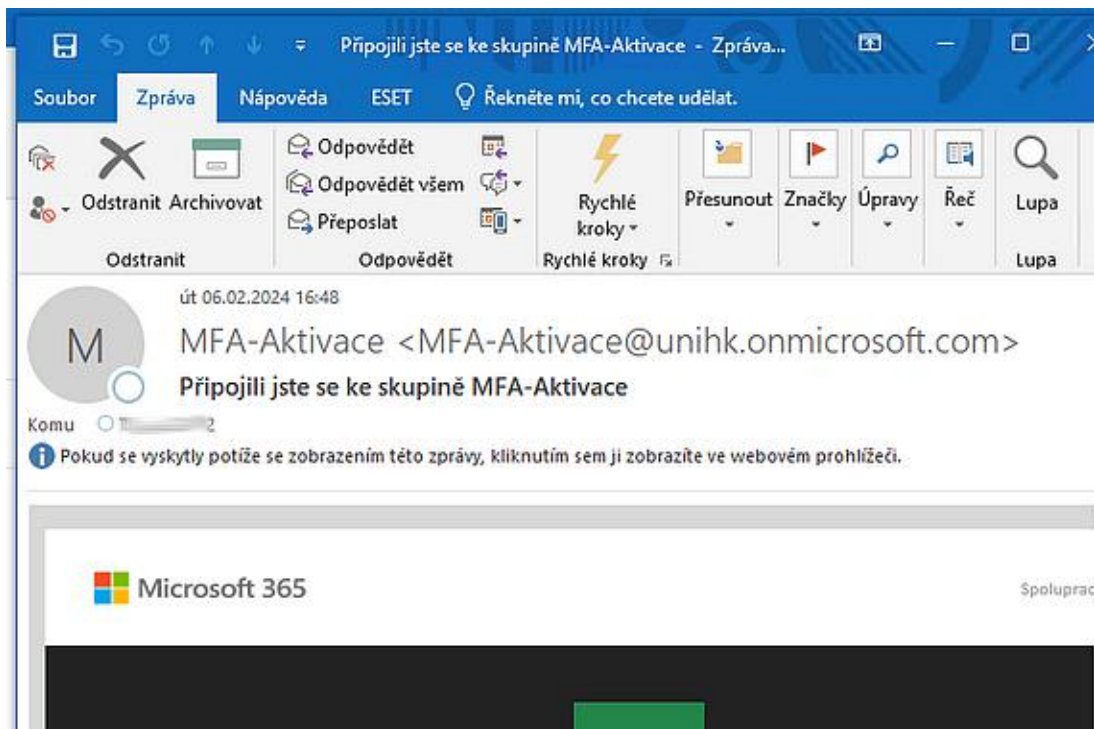
15. **Požádejte o aktivaci multifaktorové autentizace.**

Toto je důležitý krok. Teprve poté bude váš účet lépe zabezpečen.

Přidejte se do týmu **MFA-Aktivace** s kódem **ivj5agi** v [Microsoft Teams](#).

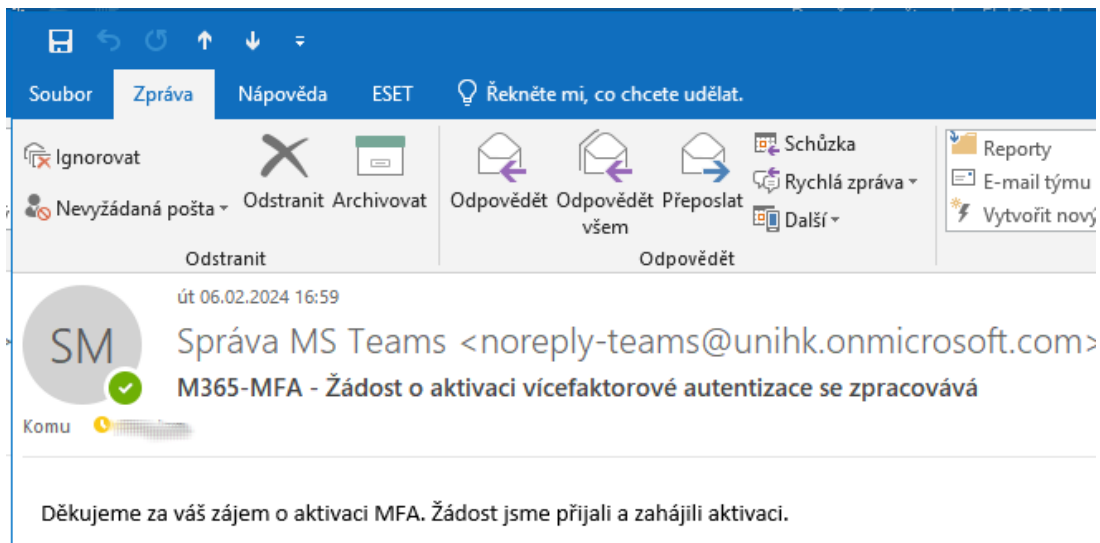


16. E-mailem obdržíte potvrzení o přidání do skupiny. Jedná se pouze o informativní e-mail, žádná další akce není třeba.



17. Dojde k zahájení zpracování žádosti. E-mailem obdržíte potvrzení a doplňující informace týkající se multifaktorové autentizace v Microsoft 365.





18. Jakmile se vícefaktorová autentizace stane aktivní, bude již přihlášení ke službám Microsoft 365 (Outlook, webové rozhraní pošty, MS Teams, Sharepoint Online a další) vyžadovat potvrzení přihlášení prostřednictvím aplikace Microsoft Authenticator nebo alternativní ověřovací metodou. Vícefaktorové ověření bude vyžadovat také e-learningový systém Blackboard Learn.

### Za jakých okolností je vícefaktorové ověřování vyžadováno

MFA je vyžadováno na základě celé řady kritérií. K ověření budete vyzváni zejména v těchto případech:

- poprvé při přihlašování do aplikace nebo webové služby po aktivaci M365 MFA
- když se přihlásíte k aplikaci nebo webovým službám Microsoft 365 na novém zařízení
- když se přihlásíte z neznámé lokality
- když se přihlásíte atypickým způsobem (běžně nevyužívaná aplikace)
- náhodné ověření, že zařízení používáte opravdu vy

V případě potíží s aktivací kontaktujte Oddělení informačních technologií prostřednictvím [helpdesku](#).