

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.
- 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.
- 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?

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



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

řidat	metodu přihlašování
0	Passkey in Microsoft Authenticator Přihlásit se pomocí rozpoznávání tváře, otisku prstu nebo PIN kódu
୍ୱ	Klíč zabezpečení nebo klíč Přihlásit se pomocí rozpoznávání tváře, otisku prstu, PIN kódu nebo klíče zabezpečení
	Klíč zabezpečení Přihlásit se pomocí zařízení USB, Bluetooth nebo NFC
٢	Microsoft Authenticator Schválit žádosti o příhlášení nebo použít jednorázové kódy
123	Hardwarový token Přihlásit se pomocí kódu z hardwarového tokenu
C	Alternativní telefon Nechat si zavolat nebo poslat textovou zprávu pro přihlášení pomocí kódu
C	Telefon do kanceláře Nechat si zavolat nebo poslat textovou zprávu pro přihlášení pomocí kódu

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

🗣 Zabe	zpečení Windows	×
Přihlast	e se pomocí sve	ého klíče
Pokud se o uloženým	hcete přihlásit k "login klíčem.	.microsoft.com", zvolte zařízení s
00 0X	Phone, iPad nebo zaříz	ení s Androidem
Další mo	ožnosti	
00 0X	iPhone, iPad nebo zai	řízení s Androidem
	Klíč zabezpečení	
	Další	Storno

Pro použití Microsoft Authenticatoru nebo textové zprávy zvolte "Další".



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

Klíč zabezpečení	>
Zvolte typ klíče zabezpečení, který máte.	
N Zařízení NFC	
N Zařízení NFC	

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

Klíč zabezpečení		×		
Připravte si svůj klíč.				
Když zvolíte Další, zobrazí se vám výzva, al do portu USB. Pak se dotkněte tlačítka nel zabezpečení, aby se dokončilo nastavovár	byste vložili klíd po senzoru na l ní vašeho zaříze	č zabezpečení klíči ení.		
Podrobnější pokyny najdete na webových stránkách výrobce klíče.				
	Zpět	Další		

6. Zvolíme, uložení vygenerovaného klíče na autentizační token

Zabezpečení Windows	×		
Zvolte, kam se má tento klíč uložit			
 ○ ○ ○ ■ iPhone, iPad nebo zařízení s Androidem ○ ■ 			
Další možnosti			
iPhone, iPad nebo zařízení s Androidem			
Klíč zabezpečení			
Další Storno			

7. Zkontrolujeme, že uvedené údaje souhlasí.



8. Potvrdíme další krok 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.



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



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

(líč zabezpečení		×
ojmenujte svůj klíč zabezpečen	í. Pomůže ho to odlišit od	l jiných klíčů
Voubikov		
TOUDIKEY		
TOUDINEY	Zrušit	Další

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

Klíč zabezpečení	×
Všechno je nastavené.	
Až se příště budete přihlašovat, můžete místo svého uživatelského jména a hesla používat klíč zabezpečení.	
Nezapomeňte podle pokynů výrobce klíče zabezpečení provést všechny další úkoly nastavení, třeba registraci otisku prstu.	
Hotovo	

- 14. Pokud se tak již nestalo, přidejte si pro jistotu záložní formu ověřování na webové stránce uvedené v kroku 1. Lze použít například <u>sms ověřování</u>. Můžete si také nainstalovat <u>Microsoft Authenticator i na další zařízení</u>, například tablet. Postupujte vždy dle instrukcí ve webovém portálu M365.
- 15. **Požádejte o aktivaci multifaktorové autentizace**. <u>Toto je důležitý krok. Teprve poté bude váš účet lépe zabezpečen.</u>

4	< > Q Hledat	🚥 🔒 Univerzita Hrade 峓 – 🗆 🗙
Q Aktivita	Týmy	···· 😌 Připojit se k týmu nebo vytvořit nový
(=) Chat	✓ Předměty	2 [°] Vytvořit tým ↓
a Zadání		🎝 Připojit se k týmu
(j) Týmy		
GHovory		
(ConeDrive	 Týmy 	

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 email, 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.

. 5 (5 ↑ ↓ =		
Soubor Zp	ráva Nápověda ESET	💡 Řekněte mi, co chcete udělat.	
িল্ল Ignorovat 🇞 Nevyžádana	á pošta v Odstranit Archivovat	Odpovědět Odpovědět Přeposlat všem	eporty E E-mail týmu Vytvořit nový
	Odstranit	Odpovědět	
út 06.02.2024 16:59 Správa MS Teams < noreply-teams@unihk.onmicrosoft.com: M365-MFA - Žádost o aktivaci vícefaktorové autentizace se zpracovává			

Děkujeme za váš zájem o aktivaci MFA. Žádost jsme přijali a zahájili aktivaci.

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 <u>helpdesku.</u>