

Co je vícefaktorová autentizace?

Luboš Pavlíček
zaměstnanec/staff

Víte, co je MFA?

MFA označuje dva způsoby přihlášení – první je, že zadáte jméno, heslo a druhý faktor (potvrzení přihlášení v Microsoft Authenticator, SMS kód či opsání časově omezeného ověřovacího kódu z aplikace). Druhý způsob je tzv. passwordless přihlášení pomocí speciální mobilní aplikace či pomocí speciálního zařízení se zadáním PINu jako je FIDO2 token – zde vůbec nezadáváte heslo.

Vícefaktorová autentizace v nastavení na VŠE neznamená opisovat dlouhý kód při každém přihlášení. Na zařízení, které běžně používáte vám stačí kód zadat při přihlášení do Insis jednoduše. Nastavení vícefaktorové autentizace zabere kolem tři minut.

Lze používat vícero metod vícefaktorového ověření?

Ano a je to doporučené řešení. Microsoft Authenticator s passwordless ověřením můžete mít nakonfigurován na více zařízeních (mobil a tablet). Můžete mít Microsoft Authenticator a na druhém zařízení aplikaci generující ověřovací kódy. Pokud používáte notebook s MS Windows, tak je vhodné nakonfigurovat na nich Windows Hello. Omezení jsou pro SMS kódy – u účtu lze mít pouze jedno telefonní číslo a toto telefonní číslo může být pouze u jednoho účtu. Čím více autentizačních prvků budete mít, tím lepší pro vás. V případě, že jeden zapomenete či ztratíte, můžete se přihlásit jinou metodou.

Kde si nastavit metodu vícefaktorové autentizace?

Na [tuto stránce](#), si můžete zobrazit a nastavit většinu metod vícefaktorové autentizace. Výjimkou je Windows Hello, kterou nastavíte nejdříve na svém počítači a poté se přihlásíte na uvedenou stránku. Pokud nějakou metodu MFA máte nastavenou, tak uvedená stránka je dostupná pouze přes MFA ověření.

Proč je nutné se na počítačích v učebnách přihlašovat s vícefaktorovou autentizací pokaždé?

Jedná se o **bezpečnostní opatření**, díky kterému chráníte nejen sebe, ale také ostatní uživatele, kteří k počítači přistupují před vámi nebo po vás.

Jaké jsou podporované metody pro vícefaktorovou autentizaci?

Microsoft Authenticator

Mobilní aplikace, která podporuje přihlášení bez hesla (opíšete dvě číslice z webu do mobilní aplikace, nutné datové spojení) a dvě varianty druhého faktoru - potvrďte přihlášení (tzv. push notifikace, nutné datové spojení) či opíšete kód z aplikace (viz ověřovací aplikace). Jedná se o nejvhodnější způsob MFA.

Klíč zabezpečení (FIDO2)

Funguje tak, že vložíte klíč zabezpečení do počítače a zadáte PIN ke klíči. Nemusíte zadávat jméno a heslo. Pro použití této metody je nutné si zakoupit klíč zabezpečení a spárovat se svým účtem v Microsoft Office 365

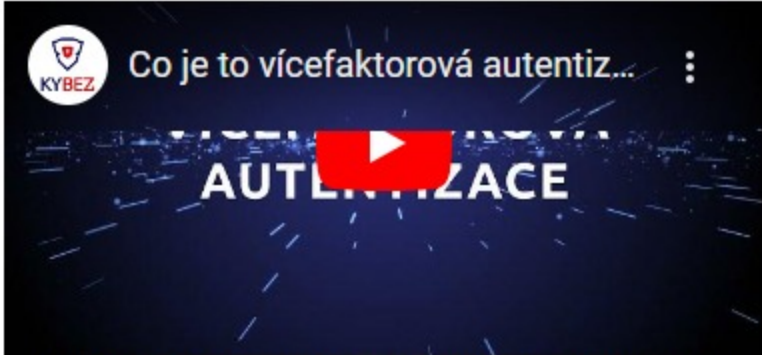
Windows Hello

Tento způsob autentizace funguje tak, že do Windows se hlásíte pomocí obličeje či otisku prstů. Poté pro přihlášení do Microsoft Office 365/Insis není potřeba zadávat jméno a heslo. Použití této metody vyžaduje kameru či čtečku otisku prstů, nutný je TPM čip. Nejdříve spárujete Windows s účtem v Microsoft Office 365.

Telefon (SMS)

Autentizace funguje jednoduše tak, že dostanete SMS s kódem. Používá se v případě, kdy uživatel nevlastní chytrý mobil či při nouzové výměně mobilu.

Vícefaktorovou autentizací se sníží riziko odcizení účtu o 96 procent.



Co je vícefaktorová autentizace? Podívejte se na video od Platforma KYBEZ, kde to vysvětlují.

Je možné použít vícefaktorovou autentizaci když nevlastním mobilní telefon?

Ano, můžete se přihlásit například pomocí bezpečnostního klíče typu FIDO2. Návod pro nastavení FIDO2 klíče naleznete [zde](#). Další možností je nosit sebou notebook a na něm mít nainstalovaného správce hesel, který umí generovat ověřovací kódy.



Zvýšení úrovně kybernetické bezpečnosti na VŠE

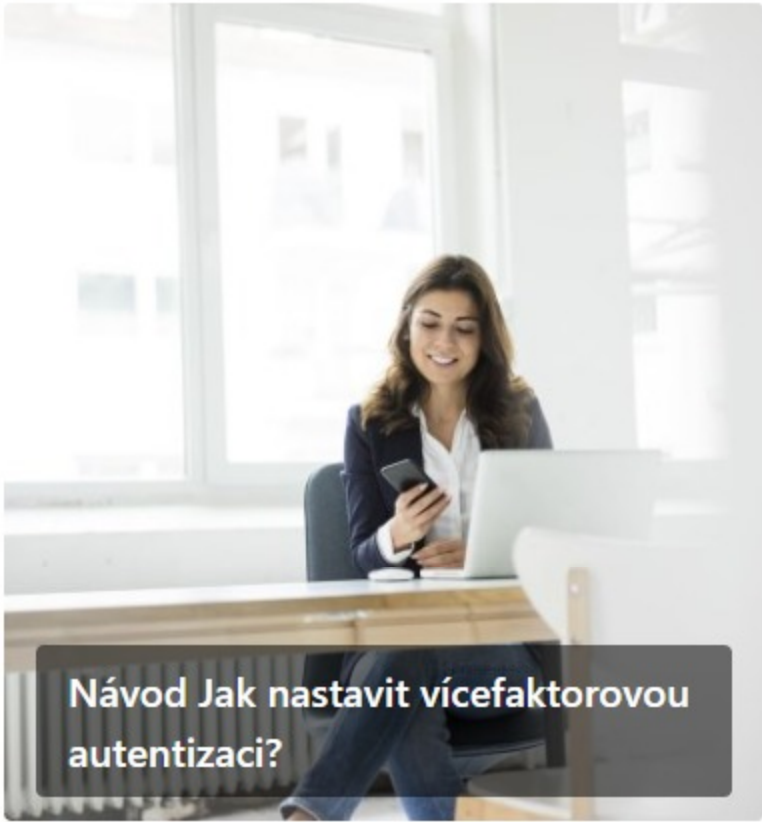
vse.sharepoint.com

Cílem zvýšení úrovně kybernetické bezpečnosti na VŠE je výrazné omezení možnosti zneužití přihlašovacích údajů. Právě na VŠE pracujeme na zavedení vícefaktorové autentizace v Insis a Office 365.

Vícefaktorová autentizace | AMI Praha

ami.cz

Vícefaktorová autentizace je pojem, který se stále více objevuje v souvislosti se zabezpečeným řízením přístupu.



Nemám nastavené MFA a nyní je již vyžadováno – co s tím?

Jste-li přihlášení do nějaké aplikace Office365 (Teams, Outlook, apod.), je šance, že budete moci pracovat dále s existujícím přihlášením. Pokud se budete přihlašovat na novém zařízení nebo vaše uložené přihlášení nebude postačovat, **budete vyzváni k přihlášení heslem** a po přihlášení heslem **budete vyzváni k nastavení MFA**. V případě mobilní aplikace Outlook budete přesměrováni na odkaz, kterým si MFA nastavíte v internetovém prohlížeči na mobilním telefonu.

Nastavení MFA

Jistým omezením v této situaci je nabídka pouze tři metod nastavení MFA – **SMS na telefon, MS Authenticator na mobilu a jiná autentizační aplikace** generující jednorázové kódy. V této situaci tedy není možné nastavit metodu bezpečnostního (FIDO) klíče. Pokud však nastavíte libovolnou z nabízených metod a přihlásíte se s nastavenou MFA, budete si poté moci nastavit i ověření pomocí bezpečnostního (FIDO) klíče (je možné mít nastaveno více MFA metod).

MS Authenticator na mobilu

- Nainstalujte si na mobil aplikaci **Microsoft Authenticator** (jiné možnosti nastavení MFA naleznete níže). Tuto aplikaci spustíte, zvolte **Přidat účet**, vyberte **Pracovní nebo školní účet** a nakonec zvolte **Naskenovat kód QR**.
- V dialogu pro nastavení MFA bude **Microsoft Authenticator** předvolen jako výchozí volba, zvolte tedy rovnou tlačítko „**Další**“ a pak ještě jednou, dokud se vám nezobrazí **QR kód**.
- Naskenujte telefonem **QR kód** z průvodce nastavení vícefaktorového ověřování. Potvrďte na mobilu testovací oznámení tlačítkem **Schválit** a pokračujte na počítači tlačítkem **Další**.
- Po nastavení druhého faktoru budete při dalším přihlašování do Office365 vyzváni k zadání kódu, který si zobrazíte v aplikaci **Microsoft Authenticator** v mobilu.

SMS na telefon

- V dialogu pro nastavení MFA klepněte ve spodní části na „**Chci nastavit jinou metodu**„. Z rozbalovacího seznamu zvolte metodu „**Telefon**„.
- Zadejte **předvolbu a telefonní číslo**, na které chcete dostávat SMS s ověřovacími kódy. **Upozornění:** *pro tuto metodu není možné použít telefonní číslo, které v rámci organizace využívá k ověřování jiný uživatel*.
- Pro ověření telefonu vám na něj bude zaslán 6-ti místný kód, který opíšete do dialogu. Po tomto kroku bude nastavení dokončeno.

Jiná autentizační aplikace na mobilu

- V dialogu pro nastavení MFA bude jako výchozí volba předvolen **Microsoft Authenticator** – zvolte tedy „**Chci použít jinou ověřovací aplikaci**„.
- Office365 vás vyzve k tomu, abyste ve vámi zvolené aplikaci **přidali nový účet** pro jednorázové kódy. Učíte tak a v dialogu Office 365 klepněte na tlačítko „**Další**„. Měl by se vám zobrazit **QR kód**, který pak naskenujete vaší mobilní aplikací.
- Poté budete požádáni o **zadání kódu** vygenerovaného vaší mobilní aplikací. Učíte tak. Tím si Office365 ověří, že párování s mobilem proběhlo úspěšně a nastavení metody ověření se dokončí.

2 osoby toto olajkovaly.

komentář

394 zobrazení

Uložit na později

0 komentáře



Napište komentář. Pokud chcete někoho zmínit, zadejte znak @.

Publikovat