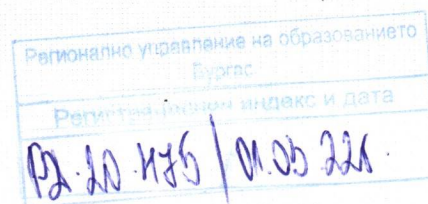




РЕПУБЛИКА БЪЛГАРИЯ
Заместник-министър на образованието и науката

№ 9105-32
01.03 2022 г.



ДО
НАЧАЛНИЦИТЕ НА РЕГИОНАЛНИТЕ
УПРАВЛЕНИЯ НА ОБРАЗОВАНИЕТО

Относно: *Опити за подвеждане на потребители за предоставяне на пароли за
достъп до edu.mon.bg.*

УВАЖАЕМА/УВАЖАЕМИ ГОСПОЖО/ГОСПОДИН НАЧАЛНИК,

Във връзка със зачестилите сигнали за опити за подвеждане на потребители да предоставят свои потребителски данни (потребителско име и/или парола) за вход в @edu.mon.bg, Ви уведомяваме следното:

1. Служители на министерството, негови отдели или изпълнители, отговорни за поддръжката на информационната инфраструктура **по никакъв начин и никога няма да поискат от Вас** да предоставяте и споделяте с тях информация относно потребителски акаунти и пароли за тях.
2. Комуникацията по електронна поща от страна на служители на министерството и неговите звена се извършва само от официални е-мейл адреси в домейните @mon.bg, @edu.mon.bg, @guo.mon.bg. Ако получите съобщения от податели, представящи се за служители на МОН, от адреси, които са от различни публични домейни, приканващи ви да споделите с тях информация за Вашите потребителско име и/или парола, или да извършите други действия с

- предоставени ви от МОН акаунти, моля незабавно да уведомите дирекция ИКТ и Звеното за мрежова и информационна сигурност на МОН.
3. В тази връзка, в бъдеще време всяка официална комуникация през електронна поща от страна на директори и учители към министерството следва да се извършва през предоставените им в домейна @edu.mon.bg служебни профили. За кореспонденция, касаеща училището, от страна на министерството ще се използва единствено електронната поща код_по_админ@edu.mon.bg.
 4. С оглед повишаване на сигурността на профилите в @edu.mon.bg, имащи разширени функции и достъп (код_по_админ@edu.mon.bg и код_по_админит@edu.mon.bg), ще бъдат предприети допълнителни технически мерки за тяхната защита, като ще бъде активирана функционалност за мултифакторна автентикация при влизане в профила и влизане в системи на МОН. Инструкции относно начина за използване на мултифакторна автентикация за тези профили са приложени към настоящето писмо.

Моля, също така за повишено внимание относно отварянето на кореспонденция, пристигнала в електронната поща със странно и нетипично съдържание, особено такава, която Ви насочва към въвеждане или смяна на паролите Ви, посещение на линкове с такава цел и др. подобни, като внимателно прочитате съобщенията и проверявате подателя и линковете в тях. Никога не отваряйте прикачени файлове в подобни съобщения, както и не достъпвайте (натискате) линкове от тях преди да сте сигурни за тяхното съдържание!

Само служители на министерството – съгласно утвърдените правила и официални канали за комуникация – могат да се обръщат към Вас във връзка с Вашите акаунти, като отново напомням, че те никога няма да поискат от Вас да предоставите информация относно паролите си или друга информация за потребителските Ви профили. При забравена или компрометирана парола или блокиран институционален акаунт единствено служител от дирекция ИКТ на МОН може да го възстанови, като при това от Вас няма да се изисква да предоставяте паролите си за достъп! В такива случаи следва да сигнализирате на help@edu.mon.bg.

В случай на съмнение, констатирани опити за подвеждане или получаване на съобщения от податели, представящи се за служители на МОН от публични домейни (например abv.bg, mail.bg, gmail.com, yahoo.com и т.н.), моля незабавно да уведомите Звеното за мрежова и информационна сигурност на МОН (тел. 02 9217 600; електронен адрес ph.ivanov@mon.bg) и/или дирекция ИКТ на МОН (тел. 02 9217 731; електронен адрес k.parashkevova@mon.bg).

Моля да разпространите информацията от настоящото писмо до всички директори на училища от Вашата област. Моля директорите на училища да уведомят учителите, относно необходимостта за опазване на сигурността на акаунтите им, като при съмнение или констатирани опити за подвеждане, незабавно да уведомяват отговорните лица в училището.

С уважение,

X

Мария Гайдарова
Заместник-министър на образованието ...
Signed by: Mariya Yordanova Gaydarova



ВЯРНО С ЕЛЕКТРОННО
ПОДПИСАНИЯ ДОКУМЕНТ

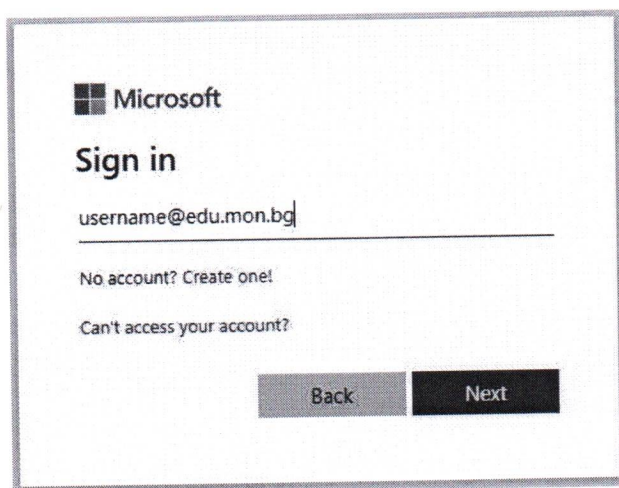
Процедура по регистрация на потребител за двуфакторна автентикация (MFA)

1. Регистрация на Вашият акаунт за двуфакторна автентикация (MFA)

Първата стъпка е да се регистрирате за двуфакторната автентикация на адрес <https://aka.ms/MFASetup>, където трябва да въведете Вашият служебен имейл и парола. Това е процедура, в която трябва да изберете метода, чрез който искате да става потвърждението и съответно да предоставите нужната информация информация.

1.1. Въвеждане на Вашия служебен имейл

При отваряне на линка от горния параграф трябва да въведете Вашият имейл



Microsoft

Sign in

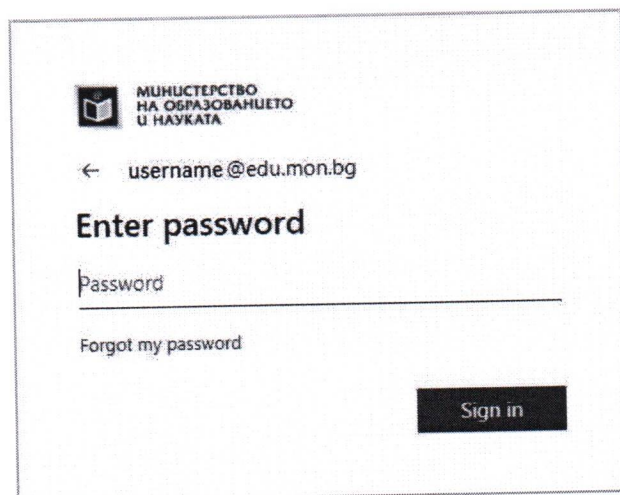
username@edu.mon.bg

No account? Create one!

Can't access your account?

Back Next

1.2. Въвеждане на Вашата парола, с която влизате в служебния имейл



МИНИСТЕРСТВО
НА ОБРАЗОВАНИЕТО
И НАУКАТА

← username@edu.mon.bg

Enter password

Password

Forgot my password

Sign in

2. Избор на метод за верификация

Методът, чрез който ще можете да потвърдите самоличността може да се реализира по два начина:

2.1. Първи вариант – чрез SMS

За да използвате този метод на удостоверяване трябва да изберете от падащото меню Authentication phone и да въведете Вашият мобилен номер, на който ще получавате SMS-ите. Когато използвате акаунта ще получавате SMS с код, който трябва да въведете в съответното поле.

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account.

Step 1: How should we contact you?

Authentication phone

Bulgaria (+359)

Method

☒ Send me a code by text message

☐ Call me

Next

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2020 Microsoft Legal | Privacy

2.2. Втори вариант - чрез приложение инсталирано на телефона

За да използвате този метод трябва да изберете от падащото меню Mobile app и да активирате радио бутона Use verification code. След това кликнете върху бутона Set up.

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account.

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

☐ Receive notifications for verification

☒ Use verification code

Set up Please configure the mobile app.

Next

To use these verification methods, you must set up the Microsoft Authenticator app.

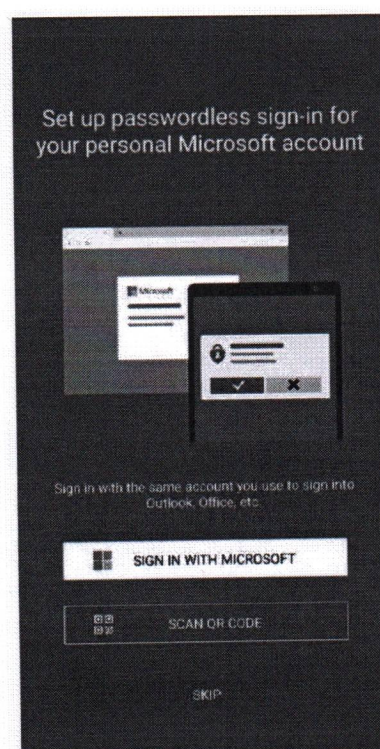
©2020 Microsoft Legal | Privacy

3. Инсталиране на приложение (Microsoft Authenticator) на Вашият мобилен телефон (smartphone)

Необходимо е да разполагате със смартфон и да можете да инсталирате приложения на него. Приложението е достъпно за Android и IOS базирани смартфони. Съответно за Android трябва да свалите и инсталирате приложението от Google Play, а за IOS от App Store. При първоначалното стартиране на приложението, то ще се нуждае от информация кой акаунт да привърже и Вие можете да го направите по два начина: чрез сканиране на QR код при регистрирането на акаунта за двуфакторна автентикация или чрез използването на акаунта Ви т.е. имейла и паролата за него.



Може да регистрирате приложението чрез сканиране на QR код или чрез използването на Вашият акаунт.



Когато се уверите, че вече имате инсталирано приложение, се връщате в браузъра и избирате една от двете опции. Първата е да получите директно нотификация, която трябва да потвърдите на телефона, а втората е да получите код, след като влезете в приложението на телефона.

За тази инструкция ще покажем опцията с известието, тъй като тя е най-използвана в световен мащаб.

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

☒ Receive notifications for verification

☐ Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up

Please configure the mobile app.

Next

На следващия екран ще Ви покаже инструкции + QR код, който трябва да сканирате през приложението на телефона.

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



If you are unable to scan the image, enter the following information in your app.

Code: 867 949 878

Url: <https://bn1eupad05.eu.phonefactor.net/pad/164373116>

If the app displays a six-digit code, choose "Next".

Next

cancel

Трябва да отворите Microsoft Authenticator, в горния десен край има три точки, натискате на тях и избирате **Добавяне на акаунт**. След това избирате Служебен или учебен акаунт и Сканиране на QR код (чрез задната камера на телефона, трябва да поставите квадратчето от сайта в квадратчето на екрана на телефона и да задържите)

Ако нямате възможност да сканирате изображението, под него има код и Url, които трябва да въведете ръчно в Microsoft Authenticator.

След като сканирате кода или въведете код и Url, натискате Next и се показва нотификация на телефона, който трябва да Одобрите.

След като сканирате кода или въведете код и Url, натискате Next и се показва нотификация на телефона, който трябва да Одобрите.

Когато успешно сте създали акаунт в приложението при стартирането му ще се появява този екран, на който ще се генерира шестцифрен код, който е валиден в рамките на 30 секунди. След изтичане на времето шестцифреният код ще се промени.

