Najczęściej zadawane pytania dotyczące logowania dwuskładnikowego – MFA (Multi-Factor Autentication)

Kiedy musze logować się za pomocą MFA?

Dwuskładnikowe logowanie (MFA) dotyczy jedynie usług Office 365.

Dlaczego podczas logowania do dziennika UONET+, aplikacji FK i KP nie musze logować się MFA?

Aplikacje dziennika elektronicznego Vulcan oraz aplikacje finansowo-księgowe i kadrowo-płacowe funkcjonują w wyodrębnionym środowisku ściśle kontrolowanym i dodatkowo zabezpieczanym przez Gdańskie Centrum Informatyczne.

Dlaczego MFA jest wymagane do aplikacji Office365?

Usługi Microsoft funkcjonują w ogólnodostępnym środowisku chmurowym, niezależnym od GCI.

Czy zawsze muszę logować się za pomocą MFA do aplikacji Office365?

Każdorazowo logując się do usług Office365 na nieużywanym wcześniej urządzeniu lub przeglądarce internetowej wymagane jest MFA.
Każdorazowo, po zmianie hasła do platformy GPE, będzie wymagane logowanie dwuskładnikowe MFA do usług Office 365.

Kiedy logowanie za pomocą MFA nie jest wymagane?

Logowanie dwuskładnikowe **nie jest** wymagane, gdy użytkownik
pozostanie zalogowany na tym samym komputerze i tej samej przeglądarce
oraz
zaznaczy opcję **Tak** przy pytaniu *Chcesz, aby Cię nie wylogowywać?* podczas logowania do usługi Office365.

Jakie są dostępne metody autoryzacji za pomocą MFA?

Autoryzacja MFA jest możliwa na 3 sposoby:

a) aplikacja **Autenticator** zainstalowana na urządzeniu mobilnym. Ta metoda nie wymaga wskazywania numeru telefonu
b) bezpłatne **połączenie telefoniczne** od Microsoft na numer telefonu wskazany podczas rejestracji MFA przez Pracownika
c) kod przesłany poprzez **SMS** na numer telefonu wskazany podczas rejestracji MFA przez Pracownika

Czy istnieją alternatywne metody uwierzytelniania?

Istnieją alternatywne metody uwierzytelniania (np. klucze FIDO2, czy tokeny sprzętowe). **Nie są rekomendowane** w środowisku GPE, ponieważ są drogie i trudne w zarządzaniu. Stosowanie kluczy lub tokenów sprzętowych jest ponadto niebezpieczne (łatwo może je przejąć osoba nieupoważniona) i niepraktyczne (łatwo zgubić, zapomnieć, itp.).

Co jeżeli zgubię telefon lub zmienię numer?

W przypadku, gdy użytkownik **zmieni numer telefonu** (który zarejestrował do autoryzacji swojego konta) lub **zgubi/zmieni telefon komórkowy** (na którym ma zainstalowaną aplikację Autenticator) jest zobowiązany zgłosić ten fakt do dyrektora JOŚW, w której pracuje. Dyrektor zakłada wówczas zgłoszenie na Helpdesku GPE: Helpdesk - Gdańska Platforma Edukacyjna

W zgłoszeniu należy uzupełnić poszczególne pola:
Typ problemu: **Wniosek o usługę**
Kategoria wniosku: **Konsultacje**
Podsystem: **MFA**
W treści zgłoszenia wskazać imię i nazwisko pracownika, któremu GCI umożliwi ponowną konfigurację MFA na koncie GPE. O realizacji zgłoszenia dyrektor zostanie poinformowany w wiadomości email (odpowiedź na założone zgłoszenie).

Komu udostępniam mój nr telefonu?

Numer telefonu jest uzupełniany przez użytkownika samodzielnie podczas procesu rejestracji uwierzytelniania dwuskładnikowego MFA. Jest on widoczny tylko dla ścisłego grona osób administrujących usługą O365 w GCI. Administratorzy mają upoważnienie do przetwarzania danych użytkowników GPE.

Gdzie znajdę instrukcje dot. włączenia MFA?

Link do instrukcji logowania MFA **za pomocą aplikacji** instalowanej na urządzeniu mobilnym
https://edu.gdansk.pl/files/mfa-authenticator.pdf
Link do instrukcji logowania MFA **za pomocą nr telefonu**
https://edu.gdansk.pl/files/mfa-telefon.pdf