

Włączanie dwuetapowej weryfikacji na koncie Microsoft® 365

Co to jest weryfikacja dwuetapowa?

Weryfikacja dwuetapowa (czasami nazywana uwierzytelnianiem wieloskładnikowym) pomaga chronić Cię, utrudniając innym osobom zalogowanie się do Twojego konta Microsoft.

Są w niej wykorzystywane dwie formy weryfikacji tożsamości: hasło i metoda kontaktu (nazywana również informacjami zabezpieczającymi).

Nawet gdy inna osoba odnajdzie Twoje hasło, nie uda jej się zalogować, jeśli nie ma dostępu do innych Twoich informacji zabezpieczających. Z tego powodu ważne jest, aby używać różnych haseł do każdego konta.

Aby więc zwiększyć bezpieczeństwo konta, możesz skonfigurować wymóg dwóch kroków logowania.

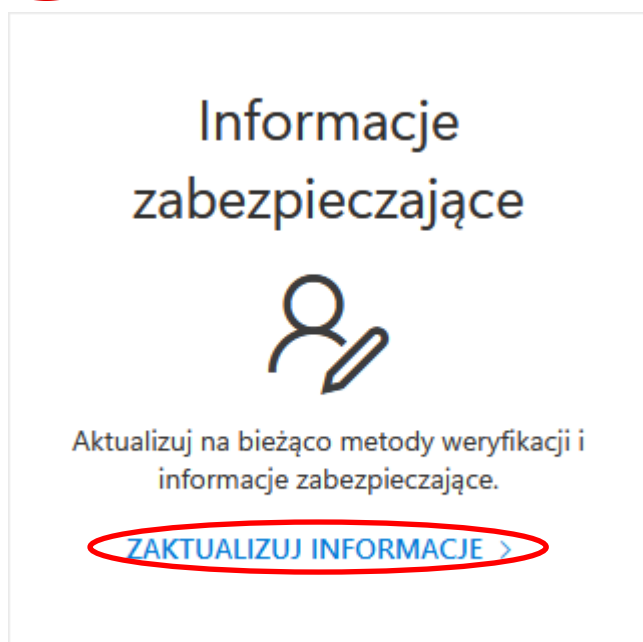
Jak włączyć weryfikację dwuetapową?

UWAGA! Na czas konfiguracji potrzebne są dwa urządzenia, komputer, na którym uruchamiamy przeglądarkę, aby zalogować się na swoje konto imienne oraz urządzenie mobilne np. telefon, gdzie instalujemy aplikację Microsoft Authenticator®, potrzebną do zeskanowania kodu QR z okna przeglądarki na komputerze.

- 1 Zaloguj się do konta Microsoft® poprzez dowolną przeglądarkę (np.: Microsoft Edge®, Firefox®) wchodząc na stronę <https://office.com/>. Następnie w prawym górnym rogu lub lewym dolnym rogu przeglądarki trzeba kliknąć na kółko z naszymi inicjałami od imienia i nazwiska wtedy pokaże się menu z opcją „Wyświetl konto”.



- 2 Następnie zostajemy przekierowani na stronę <https://myaccount.microsoft.com/?ref=MeControl> za pomocą, której klikamy w okno „Informacje zabezpieczające” -> „Zaktualizuj informacje”.



3

Pojawi się nowa strona (<https://mysignins.microsoft.com/security-info>) na której mamy możliwość dodania nowej metody logowania „Dodaj metodę logowania”.

Informacje zabezpieczające

Poniżej przedstawiono metody, których używasz w celu logowania się do konta lub resetowania hasła.

+ Dodaj metodę logowania

Hasło

Ostatnia aktualizacja:
3 miesiące temu

Zmień

Wybieramy opcję „Microsoft Authenticator”.

Dodaj metodę logowania



Microsoft Authenticator

Zatwierdzanie żądań logowania lub używanie kodów jednorazowych

123

Token sprzętowy

Zaloguj się przy użyciu kodu z tokenu sprzętowego

Microsoft Authenticator



Rozpocznij od pobrania aplikacji

Zainstaluj aplikację Microsoft Authenticator na swoim telefonie. [Pobierz teraz](#)

Po zainstalowaniu aplikacji Microsoft Authenticator na urządzeniu, wybierz przycisk „Dalej”.

[Chcę użyć innej aplikacji uwierzytelniania](#)

Anuluj

Następne

Nie klikamy jeszcze w opcję **następne**, ponieważ teraz mamy wybór tzn. albo do weryfikacji tożsamości używamy zalecanej przez firmę Microsoft® aplikacji instalowanej na urządzeniu mobilnym „**Microsoft Authenticator**®” albo instalujemy alternatywne aplikacje wybierając „Chcę użyć innej aplikacji uwierzytelniania”, jednak na chwilę obecną nie polecamy tej opcji.

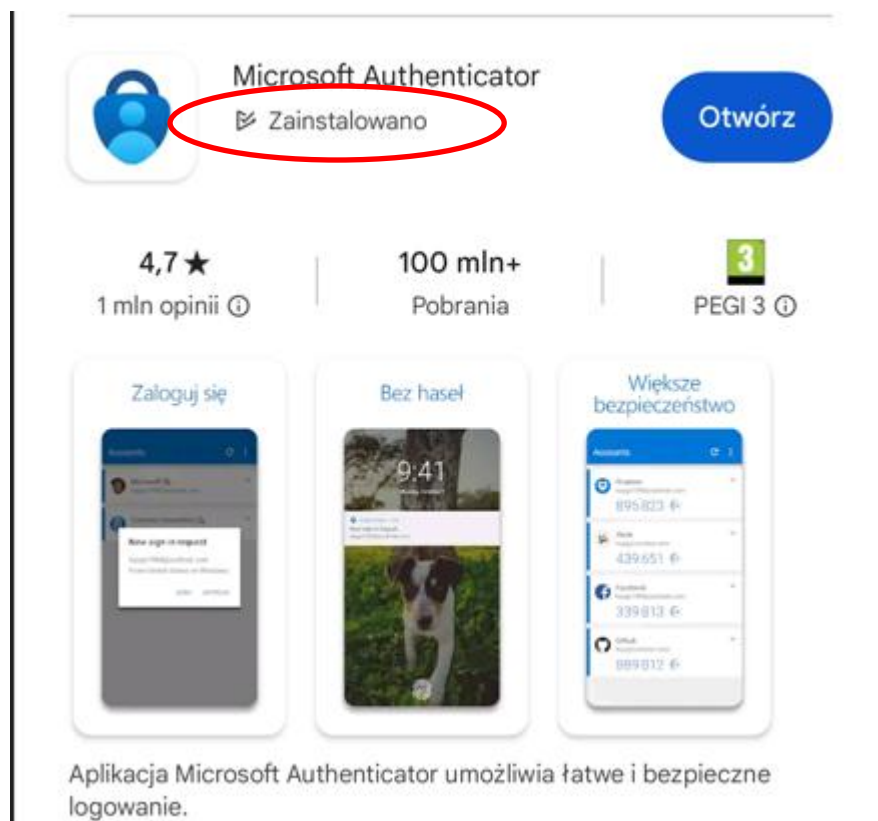
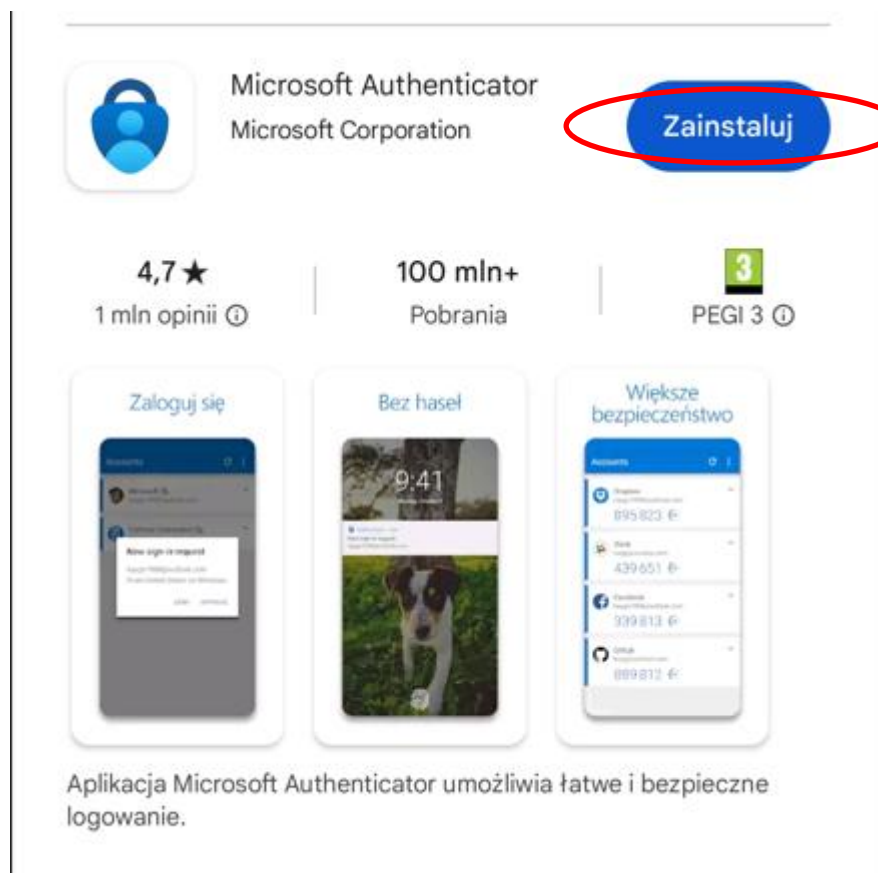
Aplikacje są dostępne za darmo dla systemów **Android**® w **Sklepie Play**® lub dla **iPhone**® w **App Store**®.

Jeśli masz już zainstalowaną aplikację **Microsoft Authenticator**®, możesz pominąć krok nr 4 i przejść do opcji dodawania konta (**krok nr 5**).

Jeśli musisz na nowo zainstalować aplikację **Microsoft Authenticator**®, postępuj zgodnie z dalszą częścią tej instrukcji, ale upewnij się, że instalujesz „Microsoft Authenticator”, a nie inną aplikację o nazwie Authenticator, ponieważ istnieje wiele aplikacji, które mają podobne nazwy.

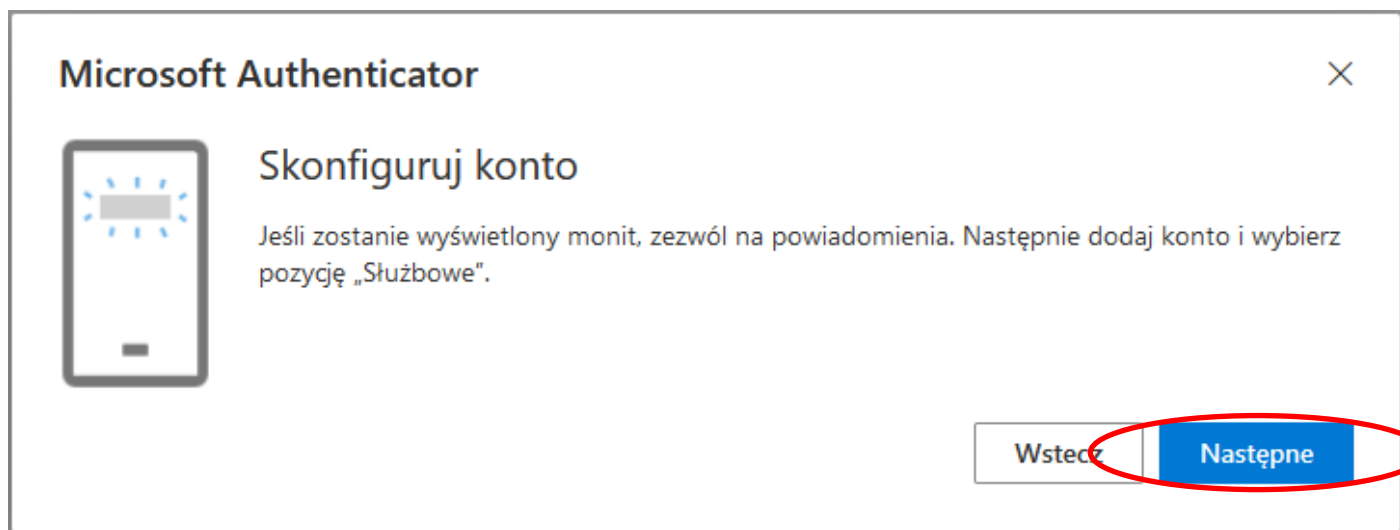
4

W celu instalacji aplikacji **Microsoft Authenticator**® w **Sklepie Play**® lub **App Store**® wyszukujemy nazwę aplikacji „Microsoft Authenticator” klikamy „Zainstaluj” i czekamy, gdy system zakończy instalację aplikacji **Microsoft Authenticator**®. Możemy kliknąć w „Otwórz” lub chwilowo nie uruchamiamy aplikacji tylko przechodzimy do okna przeglądarki na naszym komputerze.



5 Kolejnym krokiem jest dodanie naszego konta służbowego do aplikacji na urządzeniu mobilnym. W kroku nr 3 gdy zostaliśmy poproszeni o zainstalowanie **Microsoft Authenticator**® na urządzeniu mobilnym. Gdy instalacja się powiodła lub już mieliśmy zainstalowaną aplikację to dopiero teraz możemy kliknąć w przeglądarce opcję „Następne”.

Na stronie pojawi się kolejne okno z komunikatem, aby skonfigurować konto służbowe, klikamy w opcję „Następne”.

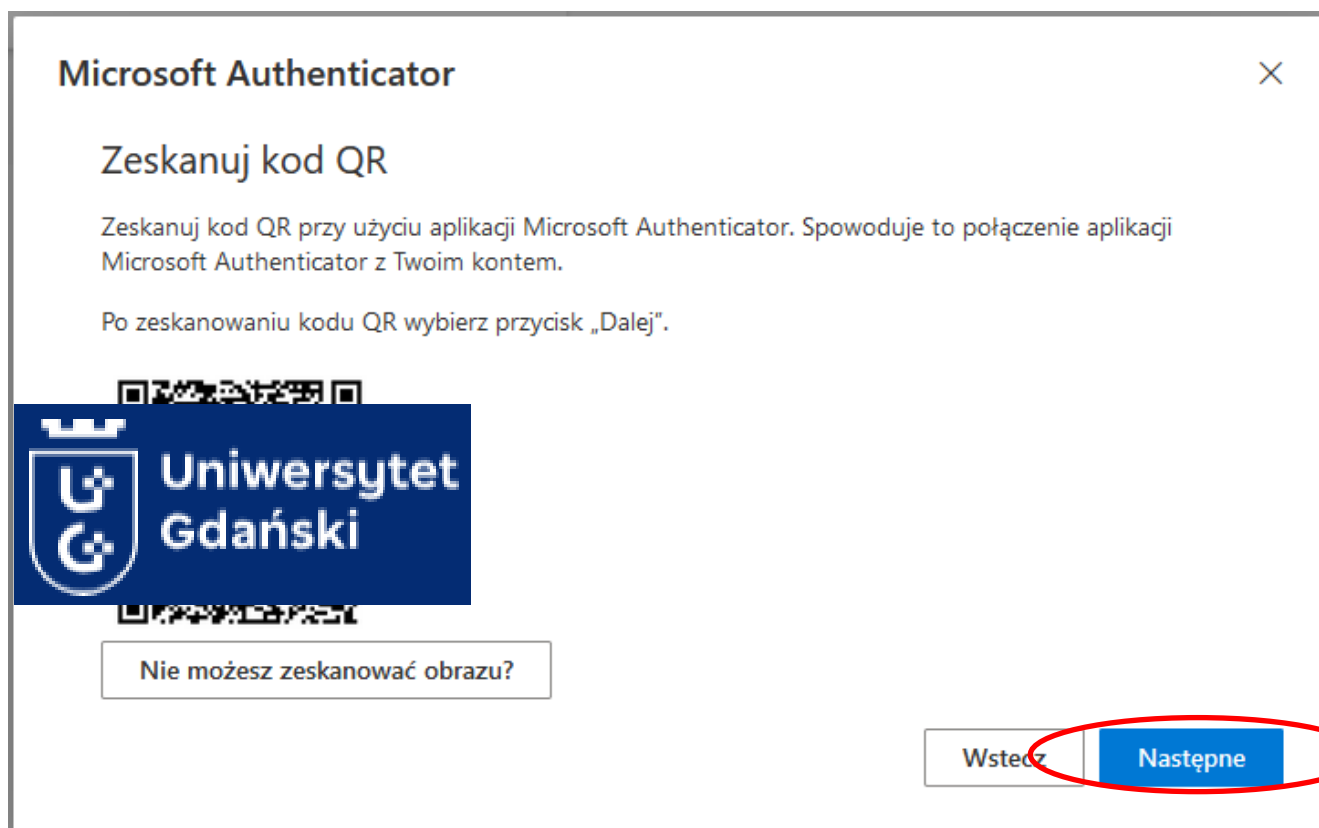


Bardzo ważna uwaga !!!

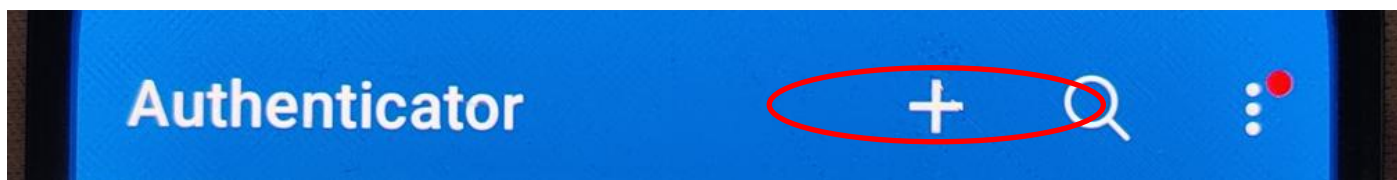
W Aplikacji **Microsoft Authenticator**® nie wybieramy opcji skanowania kodu QR. Aby dodać konto należy wybrać symbol „+”, a jako rodzaj konta wybrać „Konto służbowe”. Tylko ta metoda jest poprawna i została szczegółowo opisana poniżej.

Poniżej zobaczycie państwo przykładowy widok kodu QR w przeglądarce (ze względów bezpieczeństwa widok kodu QR został zasłonięty).

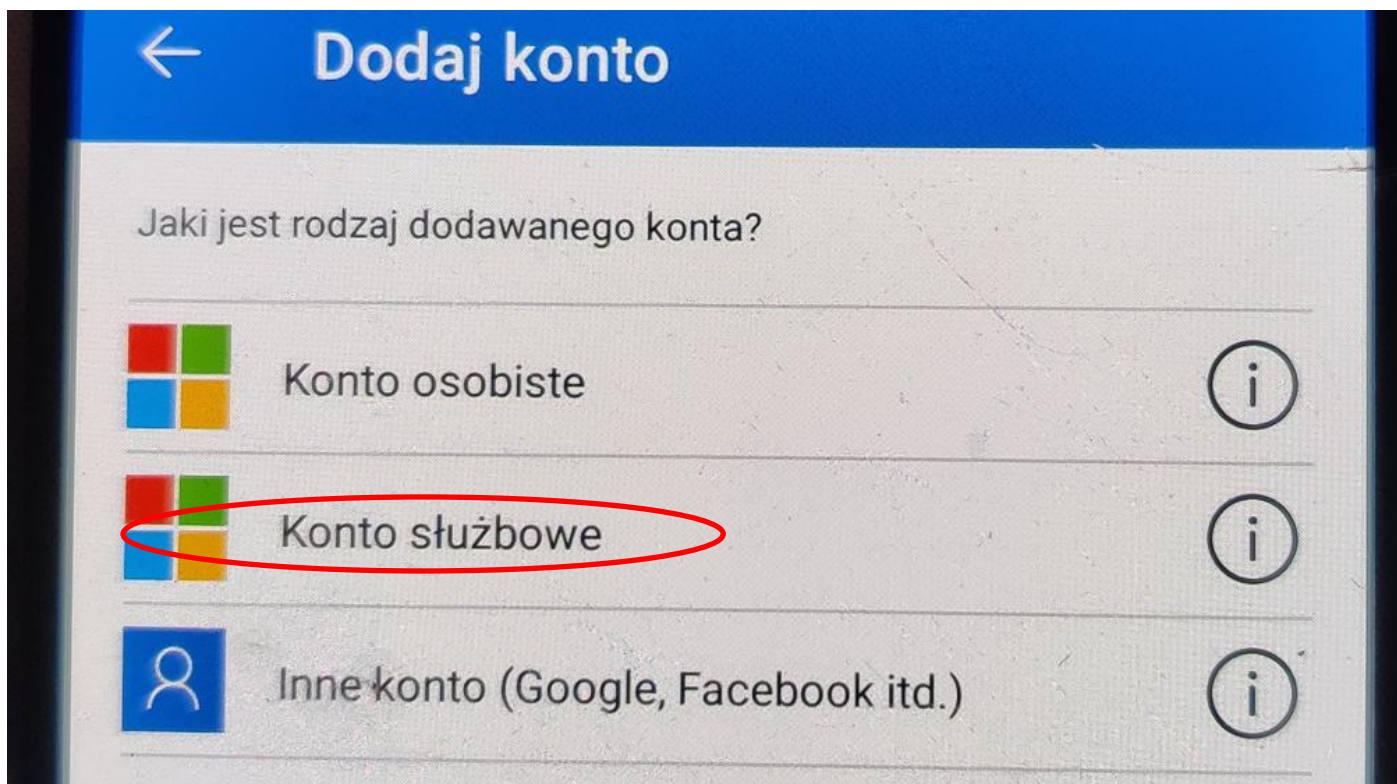
Znowu chwilowo wstrzymujemy się z kliknięciem w opcję „Następne”, ponieważ potrzebujemy zeskanować kod QR widoczny na ekranie monitora naszym urządzeniem mobilnym.



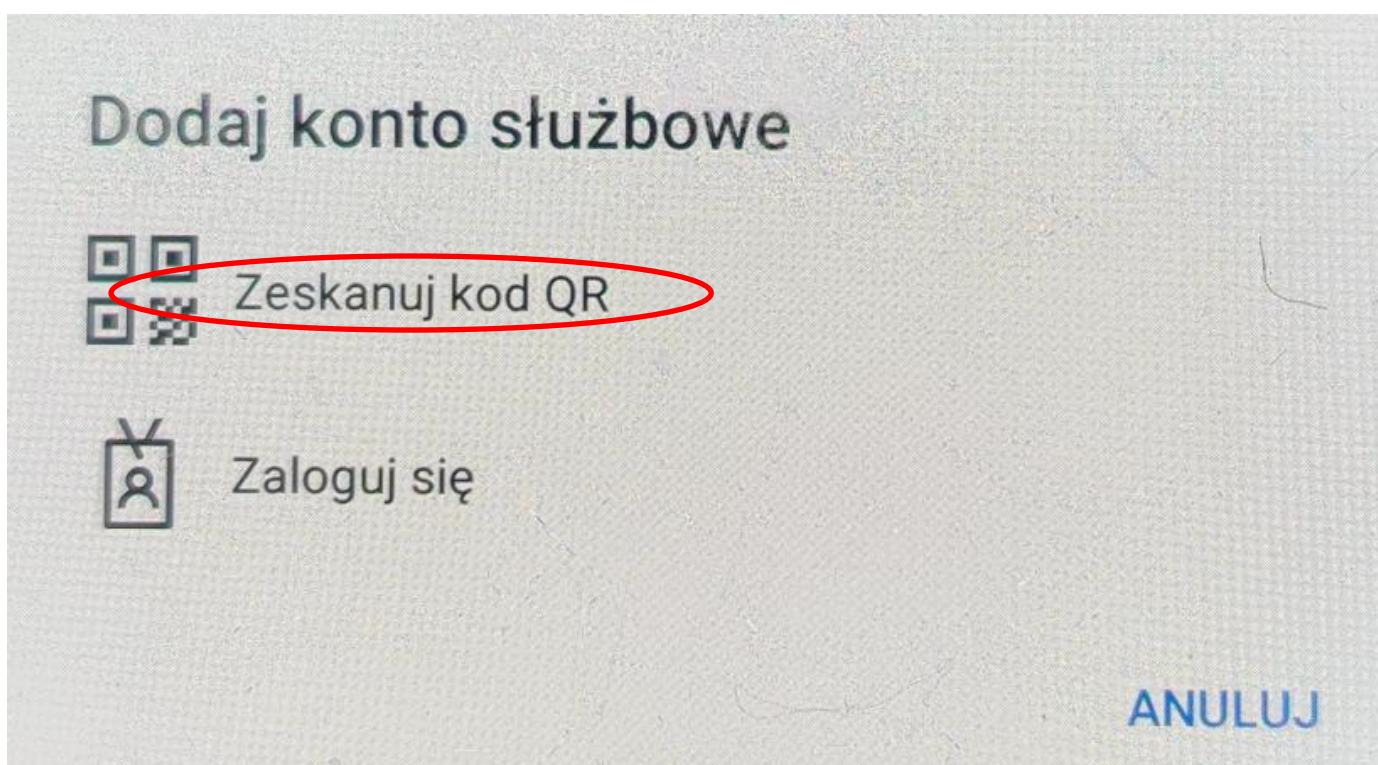
W tym celu uruchamiamy aplikację **Microsoft Authenticator**® na urządzeniu mobilnym i klikamy na plusik oznaczający chęć dodania naszego konta służbowego.



Następnie wybieramy „Konto służbowe”.



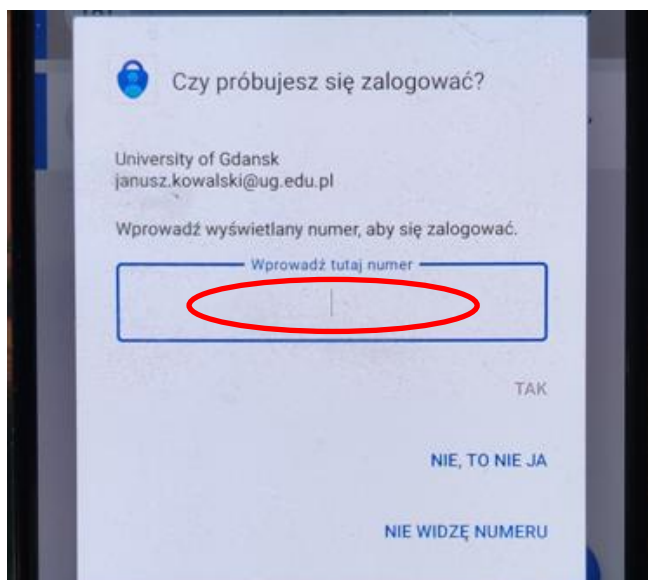
W kolejnym okienku wybieramy „Zeskanuj kod QR”, wtedy na urządzeniu mobilnym wyposażonym w aparat fotograficzny uruchomi się skaner kodów QR, wystarczy nakierować aparat na monitor naszego komputera, na którym został wcześniej wyświetlony kod QR, odczyt następuje automatycznie.



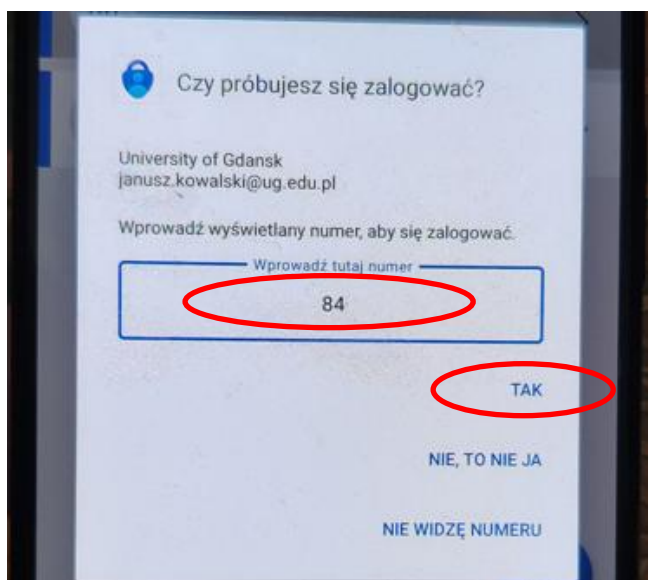
Po poprawnym zeskanowaniu kodu QR poproszeni zostaniemy o zatwierdzenie na urządzeniu mobilnym losowego numeru wyświetlonego w przeglądarce na komputerze.



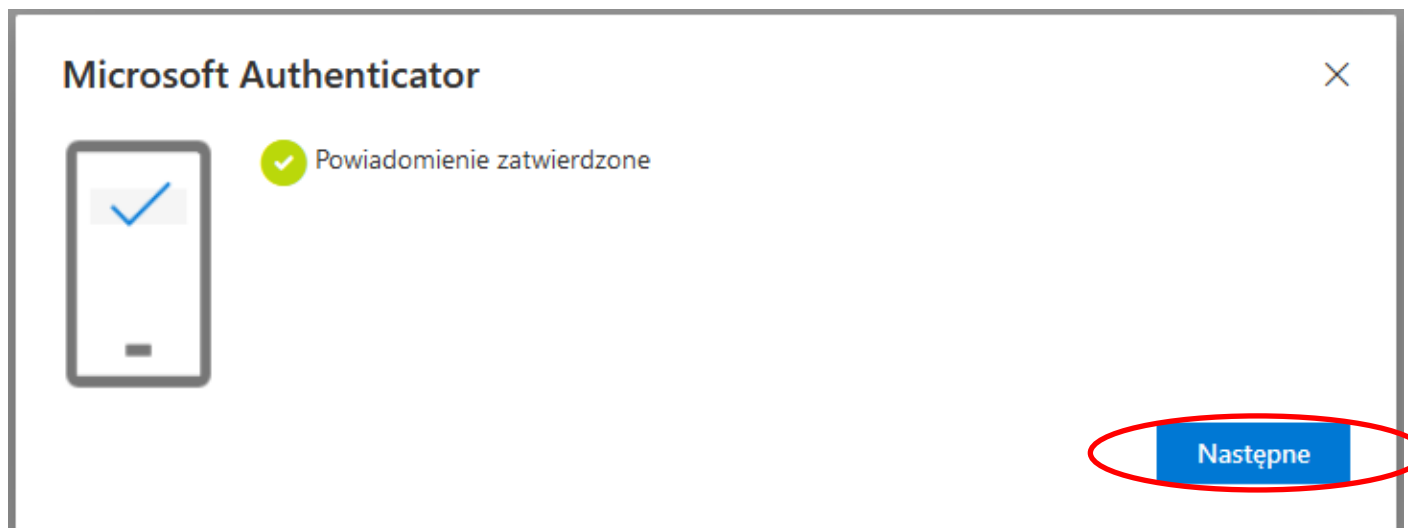
W aplikacji mobilnej **Microsoft Authenticator**® zostanie najpierw wyświetlony komunikat, aby wprowadzić podaną liczbę w odpowiednie pole,



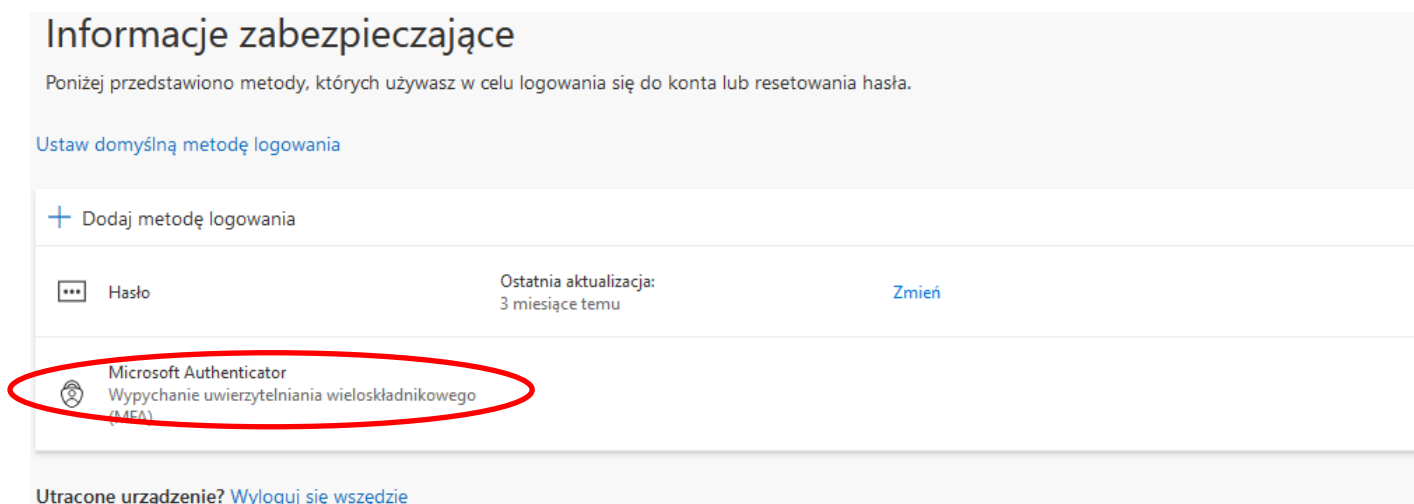
którą po wpisaniu trzeba zaakceptować klikając w przycisk „Tak” (jak widać na przykładzie jest to liczba 84),.



Gdy wszystko przebiegnie pomyślnie w przeglądarce powinien się pojawić komunikat, że aplikacja na urządzeniu mobilnym **Microsoft Authenticator**® zatwierdziła powiadomienie. Możemy kliknąć w opcję „Następne”.



W przeglądarce ponownie zobaczymy status naszych metod zabezpieczających. Tym razem dodatkowo pojawi się informacja potwierdzająca, że poprawnie skonfigurowaliśmy aplikację **Microsoft Authenticator**® i zostało w ten sposób na naszym koncie imiennym aktywowane uwierzytelnianie wieloskładnikowe.



Od tej pory w przypadku, gdy trzeba będzie potwierdzić swoją tożsamość podczas logowania do usług firmy **Microsoft**®, w aplikacji mobilnej zostaniemy poproszeni o wpisanie losowo wygenerowanego numeru celem weryfikacji naszej tożsamości.

Kiedy i dlaczego pojawiają się monity w aplikacji Microsoft Authenticator®?

- Usługa Microsoft® wykryje próbę logowania chronionego MFA.
- Na nowym urządzeniu.
- Na urządzeniu, dla którego wygasło wcześniejsze zapamiętanie (7 dni od ostatniego logowania przy użyciu MFA).

W takich przypadkach aplikacja wysyła powiadomienie, które pozwala Ci **potwierdzić lub odrzucić próbę logowania**.

Kiedy nie należy potwierdzać powiadomienia?

- **Nie Ty próbujesz się zalogować:** Jeśli nie podejmujesz w tym momencie logowania, nie potwierdzaj tożsamości.
- **Powiadomienie budzi wątpliwości:** Jeżeli wydaje się podejrzane lub nie dotyczy Twojego konta, odrzuć je.
- **Powiadomienia są częste i niepokojące:** Jeśli dostajesz powiadomienia, które nie mają związku z Twoimi działaniami, może to być oznaka problemu z bezpieczeństwem konta. W takim przypadku zgłoś to do administratora systemu.

Co warto wiedzieć na temat używania MFA i aplikacji MS Authenticator®

- Stosowanie dwuetapowej autoryzacji (MFA) jest wymagane przy każdym logowaniu do usług Microsoft® 365 spoza sieci uniwersyteckiej.
Wyjątek stanowi sytuacja, gdy podczas logowania w aplikacji Microsoft Authenticator® zaznaczono opcję zapamiętania danego urządzenia na okres 7 dni.
- Nie należy odinstalowywać aplikacji Microsoft Authenticator® ze smartfona – jest ona niezbędna do codziennego korzystania z konta uniwersyteckiego.
Odinstalowanie aplikacji (np. przez pomyłkę) i ponowne jej zainstalowanie na tym samym urządzeniu wymaga ponownej konfiguracji, czyli ponownego połączenia aplikacji z kontem Microsoft® 365.
Informacje dotyczące konfiguracji MFA są unikalne dla każdego urządzenia i każdej instalacji aplikacji.
- Aplikację Microsoft Authenticator® można zainstalować i skonfigurować na więcej niż jednym urządzeniu mobilnym (np. smartfonie i tablecie). Jest to rozwiązanie zalecane – w przypadku awarii lub braku dostępu do jednego urządzenia umożliwia zalogowanie się przy użyciu drugiego, wcześniej skonfigurowanego urządzenia. Dodatkowo pozwala to na dodanie nowego urządzenia (np. w miejsce uszkodzonego) z wykorzystaniem dwuetapowego logowania na urządzeniu zapasowym.
- W sytuacji utraty urządzenia z zainstalowaną aplikacją Microsoft Authenticator® (np. awaria, zgubienie, kradzież) konieczny jest kontakt z Centrum Informatycznym w celu usunięcia utraconego urządzenia i wymuszenia ponownej konfiguracji metody logowania przy kolejnym dostępie do usług Microsoft® 365.

Zawsze, jeśli masz jakiegokolwiek wątpliwości skontaktuj się z Sekcją Helpdesk tel. 58-523-25-88