

STUDENCI REKRUTUJĄCY SIĘ POZA SYSTEMEM INTERNETOWEJ REKRUTACJI

Aby zalogować się po raz pierwszy do usługi Microsoft 365, należy w pierwszej kolejności zalogować się na stronie panel.amu.edu.pl.

Jako loginu należy użyć pierwszego członu swojego adresu e-mail.

Jeżeli adres e-mail to ab12345@st.amu.edu.pl, to na stronie <https://panel.amu.edu.pl> należy się zalogować jako ab12345. W polu „hasło” należy wpisać tymczasowe hasło.

Login i tymczasowe hasło zostaną przesłane na prywatne skrzynki mailowe natychmiast po utworzeniu konta.



The screenshot shows the login interface for the UAM User Panel. At the top left is the UAM logo (a stylized eagle). To its right, the text reads "UNIwersYTET IM. ADAMA MICKIEWICZA W POZNANIU" and "Panel Użytkownika". Below this is a language selector button labeled "EN". The main heading is "LOGOWANIE DO PANELU". Underneath, there is a section titled "Informacje o koncie" containing two input fields: "Nazwa Użytkownika:" and "Hasło:". Below these fields is a "Zaloguj" button. At the bottom of the page, there is a copyright notice: "© Copyright 2013 - Centrum Informatyczne Uniwersytetu im. Adama Mickiewicza w Poznaniu - Wszelkie prawa zastrzeżone." and a link to "Instrukcja Logowania Użytkownika".

Po zalogowaniu się do Panelu, wyświetli się okno, w którym należy dwukrotnie wpisać nowe hasło zgodne z wymogami bezpieczeństwa. Wymagania są podane poniżej formularza zmiany hasła.

Należy zapisać zmiany i wylogować się.



LOGOWANIE DO APLIKACJI MICROSOFT 365

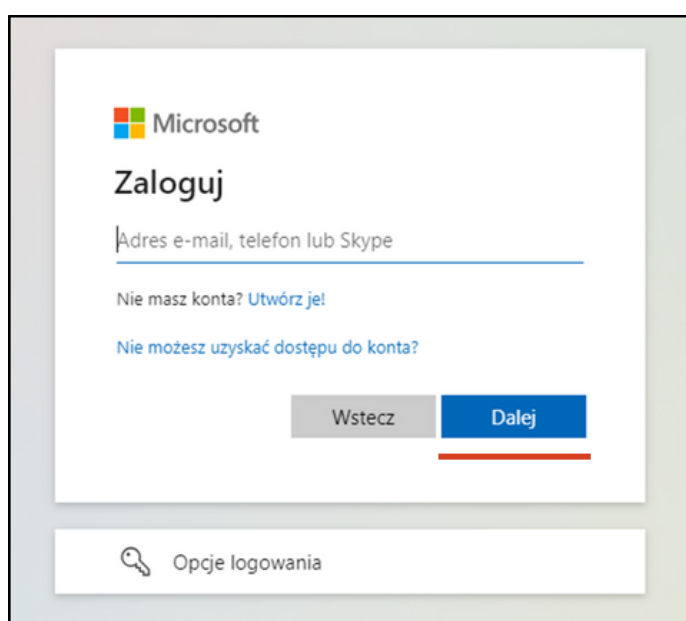
Otwieramy w przeglądarce stronę <https://www.office.com>.

Wybieramy przycisk “Zaloguj się”.



W oknie logowania, wpisujemy swój adres (login@st.amu.edu.pl) i ustawione hasło.

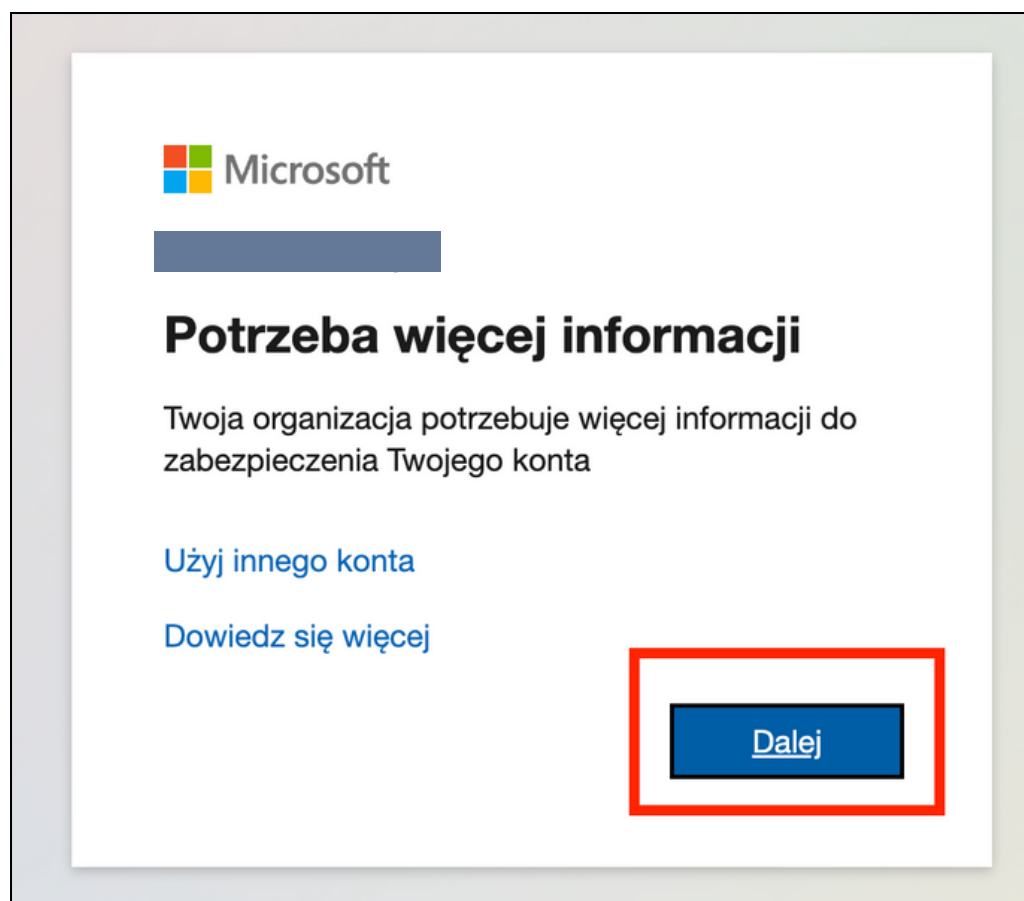
Klikamy przycisk “dalej”.



Każde konto ma włączone uwierzytelnianie wieloskładnikowe. Konfigurując dodatkowe potwierdzenie, trzeba dodać do logowania na swoim koncie usługi Microsoft 365 dodatkową warstwę zabezpieczeń. Na przykład najpierw wprowadzić hasło, a po wyświetleniu monitu wpisać także dynamicznie wygenerowany kod weryfikacyjny dostarczony przez aplikację uwierzytelniania lub wysłany na telefon w formie wiadomości SMS.

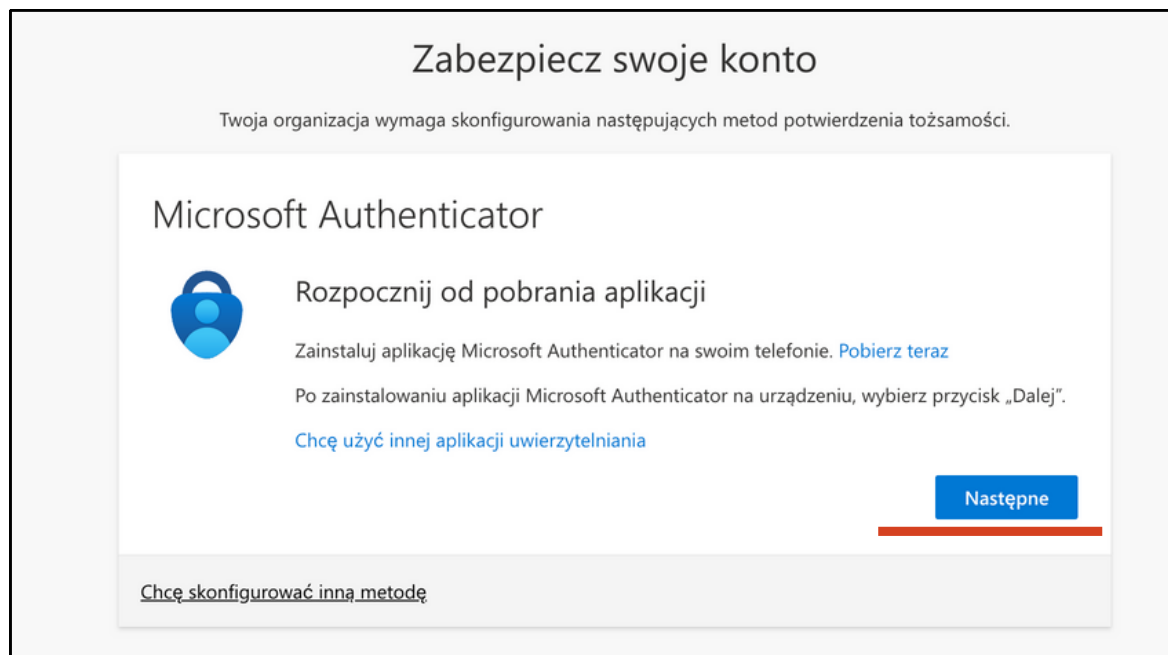
Logujemy się do usługi Microsoft 365 w zwykły sposób — za pomocą konta studenckiego i hasła. Po wybraniu pozycji “Zaloguj” zostanie wyświetlony monit o podanie dodatkowych informacji.

Potwierdzamy przyciskiem “Dalej”.

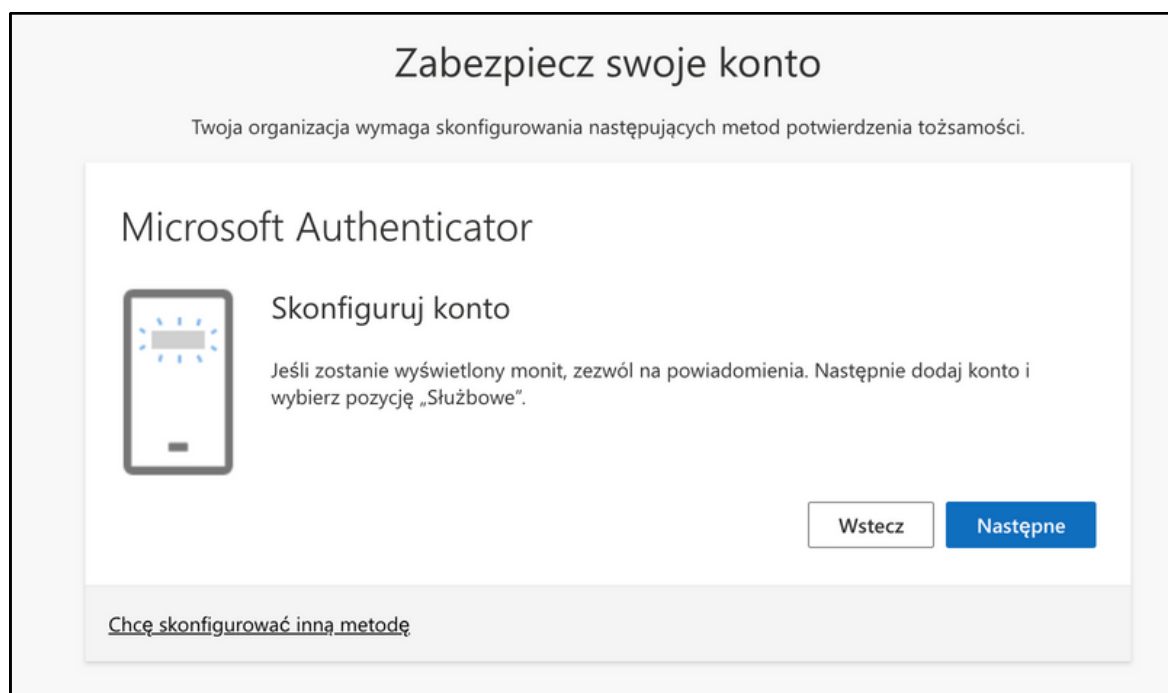


Możemy pobrać aplikację do uwierzytelnienia na swój telefon komórkowy lub wybrać inną metodę konfiguracji - sms na telefon.

WARIANT 1 - konfiguracja aplikacji Microsoft Authenticator.



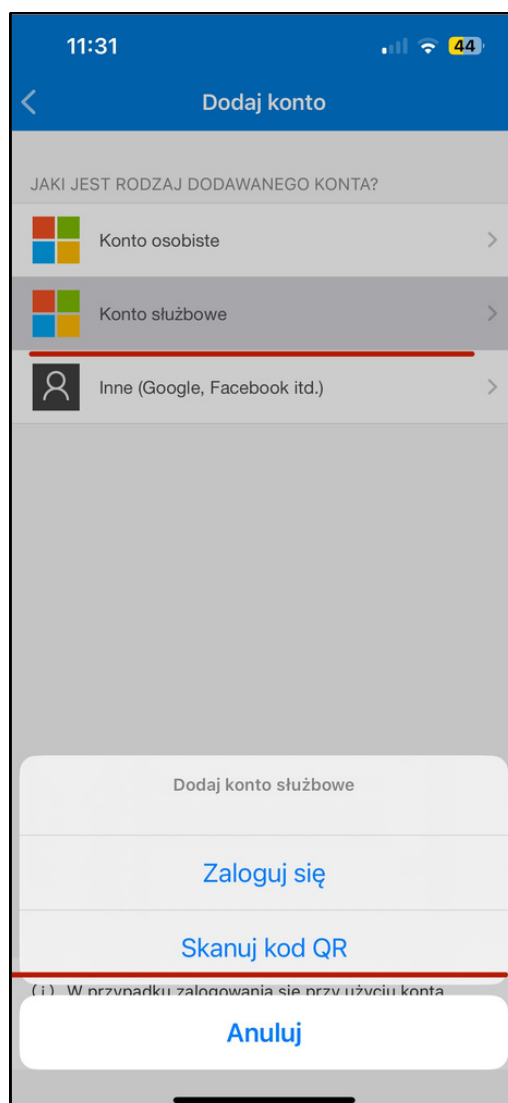
Postępujemy według komunikatów na ekranie.



Instalujemy na telefonie aplikację Microsoft Authenticator. Zgadza się, aby aplikacja wysyłała nam powiadomienia w postaci wyskakujących komunikatów typu push.

W aplikacji klikamy na ikonę “+” i dodajemy konto służbowe. Następnie wybieramy opcję skanowania kodu QR.

Po zeskanowaniu kodu, dane automatycznie zostaną zsynchronizowane, a konto przyłączone do aplikacji.



Skanujemy telefonem kod QR i postępujemy według komunikatów na ekranie i telefonie.

Zabezpiecz swoje konto

Twoja organizacja wymaga skonfigurowania następujących metod potwierdzenia tożsamości.

Microsoft Authenticator

Zeskanuj kod QR

Zeskanuj kod QR przy użyciu aplikacji Microsoft Authenticator. Spowoduje to połączenie aplikacji Microsoft Authenticator z Twoim kontem.

Po zeskanowaniu kodu QR wybierz przycisk „Dalej”.



Nie możesz zeskanować obrazu?

Wstecz

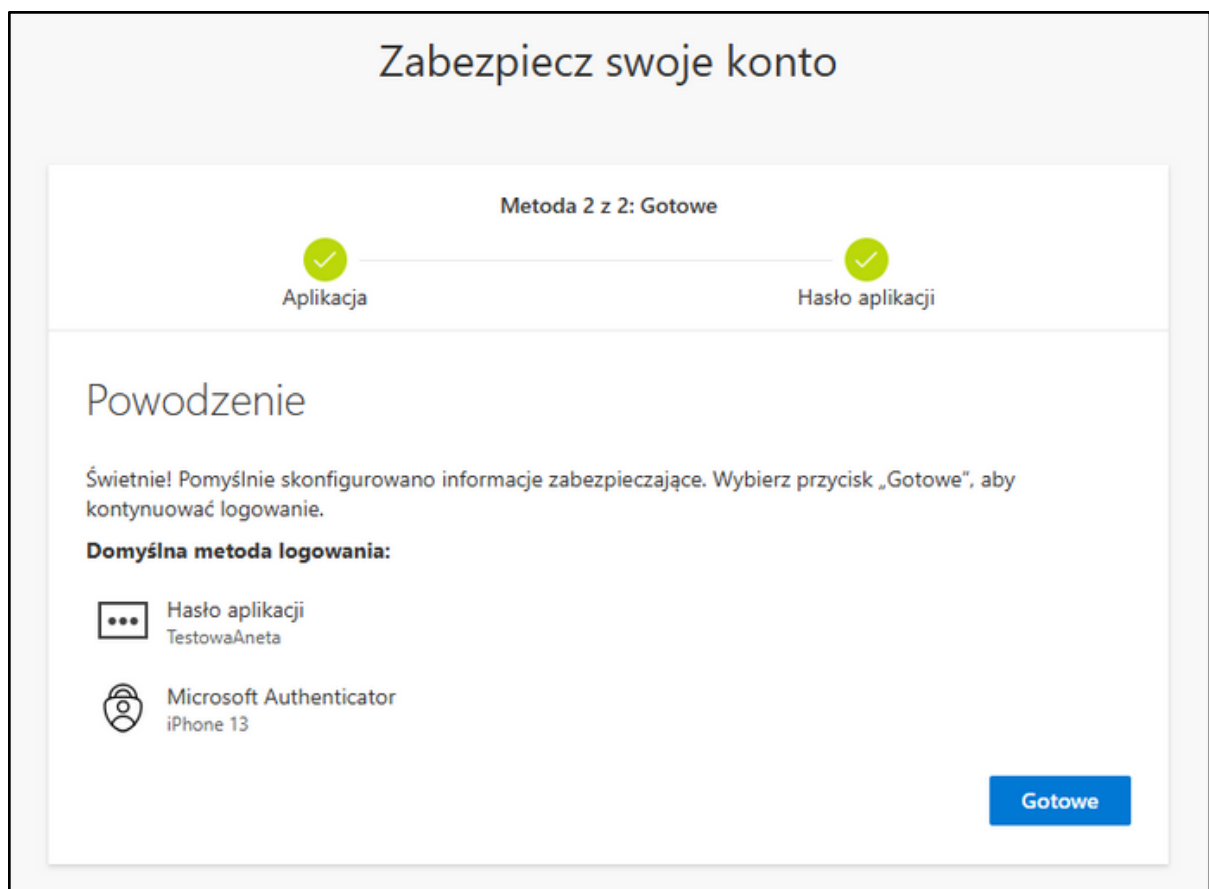
Następne

[Chcę skonfigurować inną metodę](#)



UWAGA! W ostatnim etapie konfiguracji system wygeneruje dla nas dodatkowe hasło. Prosimy je zachować w bezpiecznym miejscu. Jest to bezpieczne hasło, które umożliwi zalogowanie do usług Microsoft w przypadku utraty wszystkich innych możliwości logowania.

Po zakończeniu konfiguracji, na ekranie pojawi się komunikat.



Zabezpiecz swoje konto

Metoda 2 z 2: Gotowe

Aplikacja Hasło aplikacji

Powodzenie

Świetnie! Pomyślnie skonfigurowano informacje zabezpieczające. Wybierz przycisk „Gotowe”, aby kontynuować logowanie.

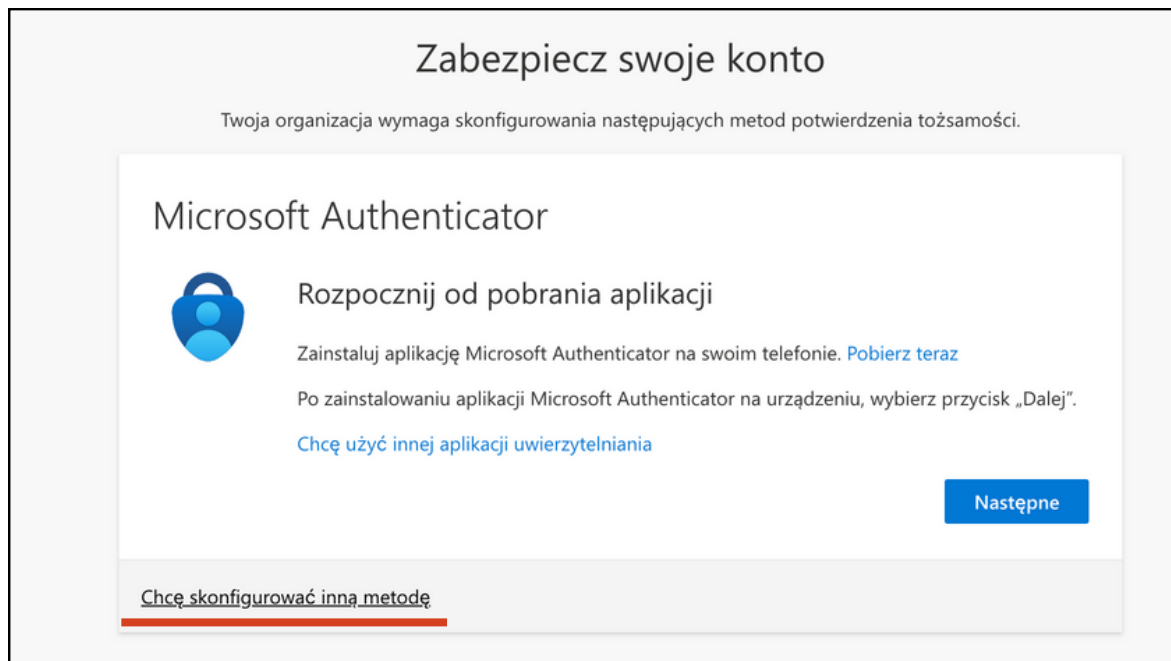
Domyślna metoda logowania:

- Hasło aplikacji
TestowaAneta
- Microsoft Authenticator
iPhone 13

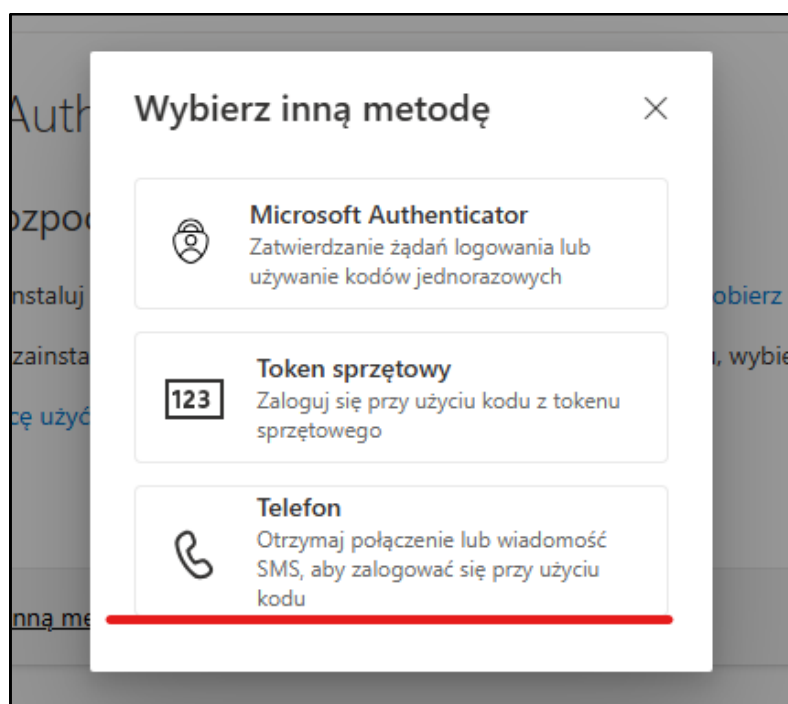
Gotowe



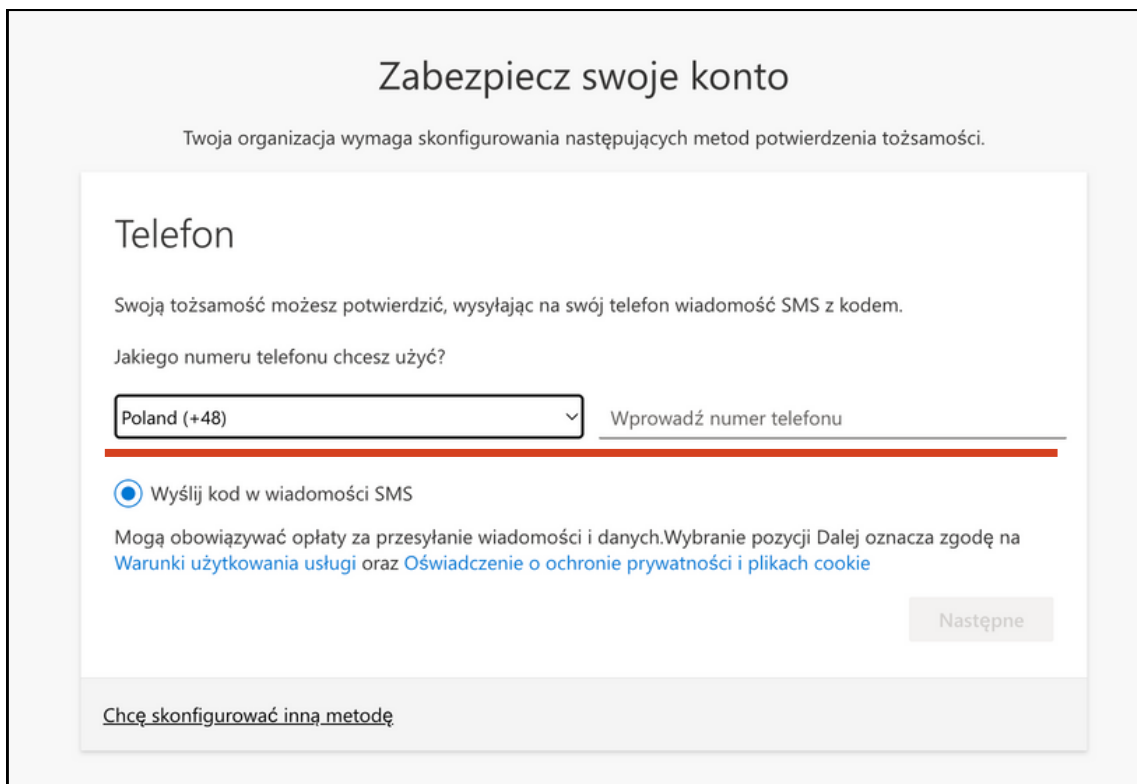
WARIANT 2 - sms na telefon.



Po wybraniu “Chcę skonfigurować inną metodę”, w nowym oknie wybieramy metodę “Telefon”.



Wybieramy numer kierunkowy telefonu oraz wprowadzamy numer telefonu, na który ma przyjść kod weryfikacyjny.



Zabezpiecz swoje konto

Twoja organizacja wymaga skonfigurowania następujących metod potwierdzenia tożsamości.

Telefon

Swoją tożsamość możesz potwierdzić, wysyłając na swój telefon wiadomość SMS z kodem.

Jakiego numeru telefonu chcesz użyć?

Poland (+48) Wprowadź numer telefonu

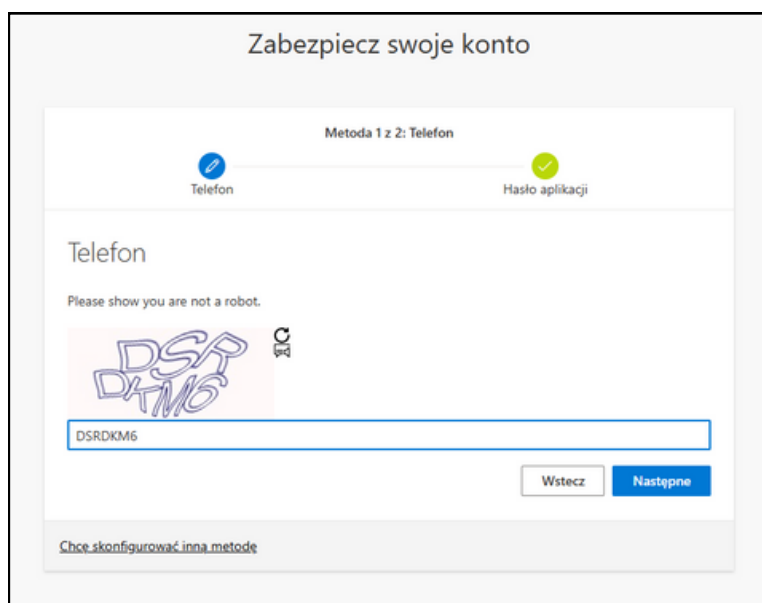
☒ Wyślij kod w wiadomości SMS

Mogą obowiązywać opłaty za przysyłanie wiadomości i danych. Wybranie pozycji Dalej oznacza zgodę na [Warunki użytkowania usługi](#) oraz [Oświadczenie o ochronie prywatności i plikach cookie](#)

Następne

[Chcę skonfigurować inną metodę](#)

Potwierdzamy, że nie jesteśmy robotami.



Zabezpiecz swoje konto

Metoda 1 z 2: Telefon

Telefon Hasło aplikacji

Telefon

Please show you are not a robot.

DSR DTM6

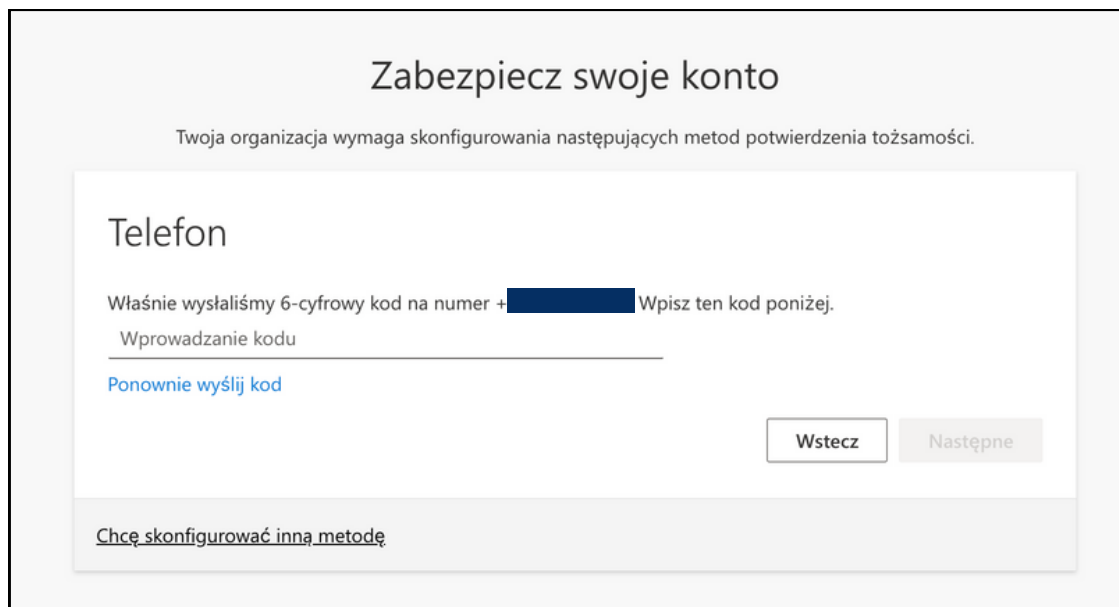
DSRDKM6

Wstecz Następne

[Chcę skonfigurować inną metodę](#)



W nowym oknie wpisujemy otrzymany w wiadomości sms kod.



Zabezpiecz swoje konto

Twoja organizacja wymaga skonfigurowania następujących metod potwierdzenia tożsamości.

Telefon

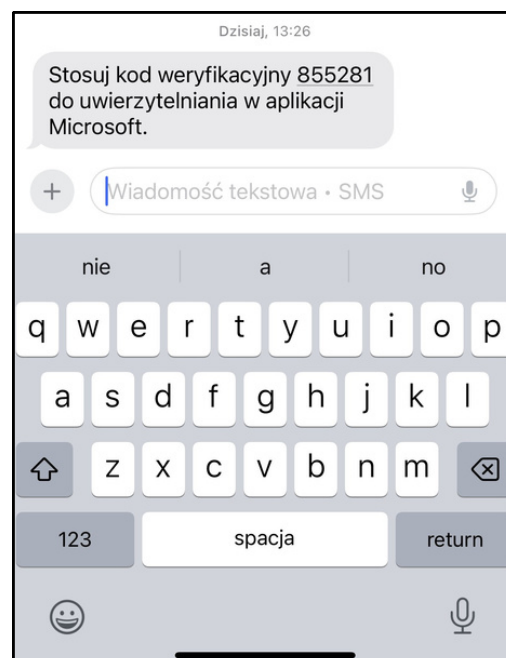
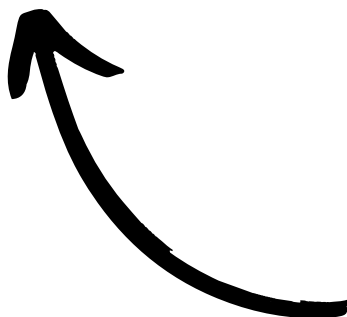
Właśnie wysłaliśmy 6-cyfrowy kod na numer + [redacted] Wpisz ten kod poniżej.

Wprowadzanie kodu

[Ponownie wyślij kod](#)

[Wstecz](#) [Następne](#)

[Chcę skonfigurować inną metodę](#)



Po poprawnej konfiguracji, otrzymujemy komunikaty z informacją o powodzeniu.

Zabezpiecz swoje konto

Twoja organizacja wymaga skonfigurowania następujących metod potwierdzenia tożsamości.

Telefon

✓ Zweryfikowano wiadomość SMS. Twój telefon został pomyślnie zarejestrowany.

Następne

Zabezpiecz swoje konto

Twoja organizacja wymaga skonfigurowania następujących metod potwierdzenia tożsamości.

Powodzenie

Świetnie! Pomyślnie skonfigurowano informacje zabezpieczające. Wybierz przycisk „Gotowe”, aby kontynuować logowanie.

Domyślna metoda logowania:

 Telefon

Gotowe



UWIERZYTELNIANIE WIELOSKŁADNIKOWE

LOGOWANIE Z UŻYCIEM APLIKACJI

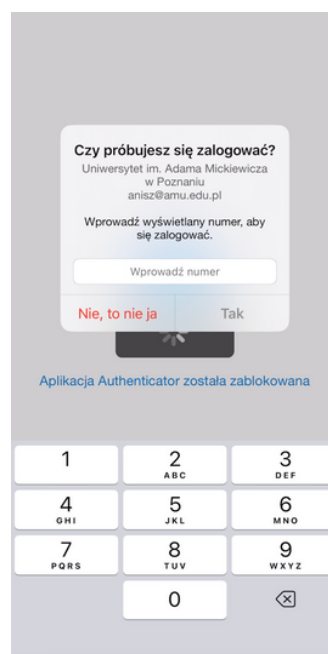
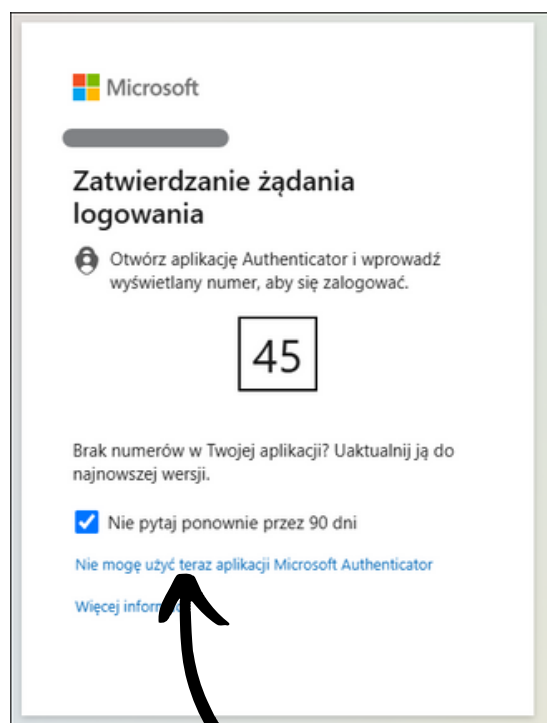
Konfiguracje przeprowadzamy tylko raz.

Od tego momentu, podczas logowania na konto i do wszystkich aplikacji Microsoft, uruchomione zostanie dodatkowe potwierdzenie w postaci kodu wygenerowanego losowo.

Po wpisaniu adresu e-mail i hasła podczas logowania, pojawi się dodatkowe okno, a w nim losowo wygenerowana liczba.

Zaprezentowaną na ekranie liczbę należy wpisać w aplikacji Microsoft Authenticator w telefonie. UWAGA! W konieczne jest włączenie w telefonie powiadomień typu push, czyli wyskakujących komunikatów.

Proces logowania zostanie zakończony.



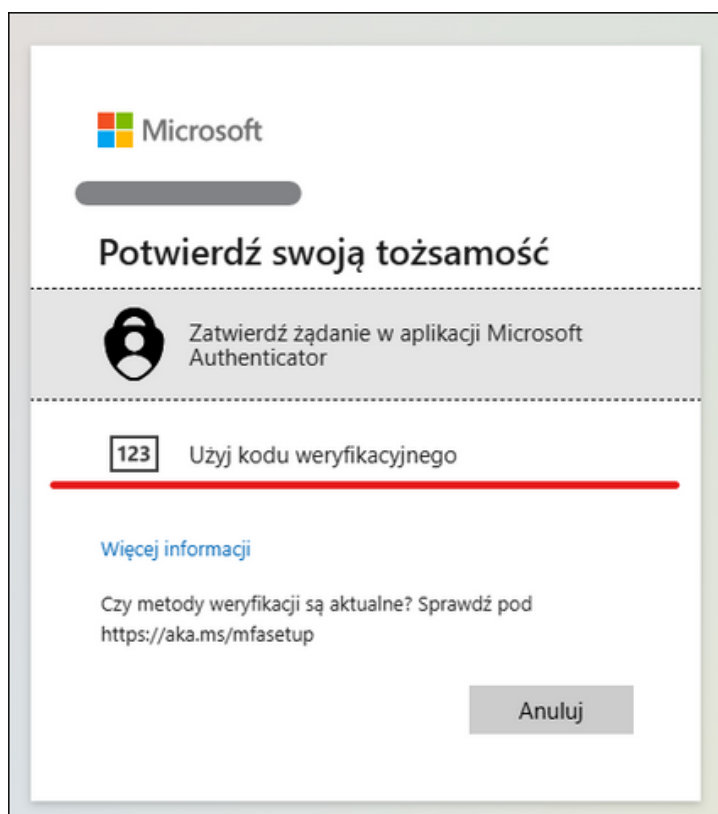
W celu zwiększenia bezpieczeństwa, zalecamy odznaczenie funkcji.



Centrum Informatyczne UAM
helpdesk@amu.edu.pl
tel. 61 829 2670

Jeśli występują problemy z pojawiającym się kodem, możemy skorzystać z opcji “Nie mogę teraz użyć aplikacji Microsoft Authenticator”.

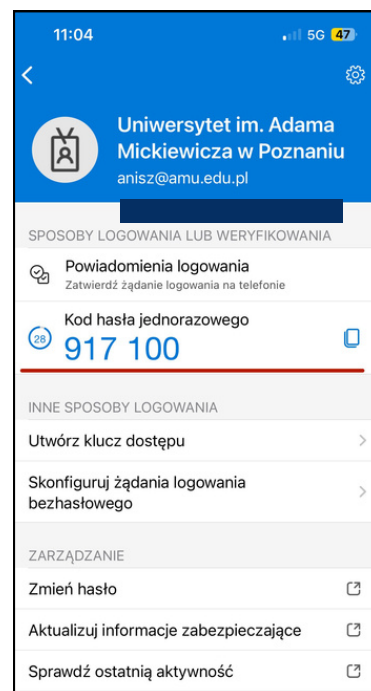
Pojawi się nowe okno, w którym możemy wybrać “Użyj kodu weryfikującego” i wprowadzić kod ręcznie wygenerowany w aplikacji na telefonie. Kod jest aktywny 30 sekund i po tym czasie generowany jest nowy kod.



Widok z komputera



Widok z telefonu



LOGOWANIE Z UŻYCIEM KODU SMS

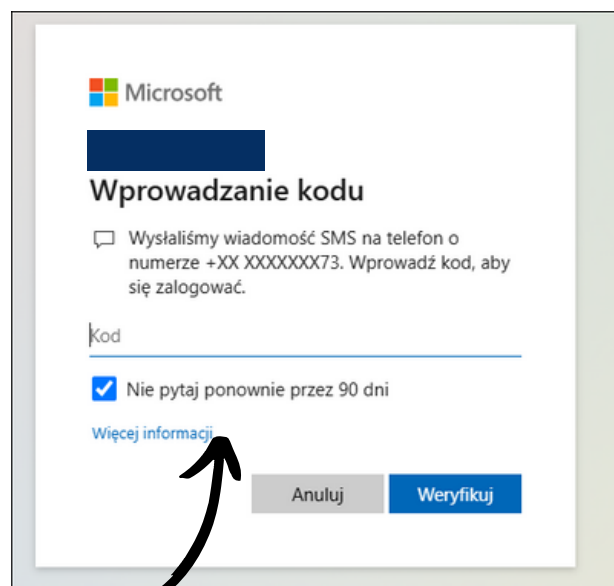
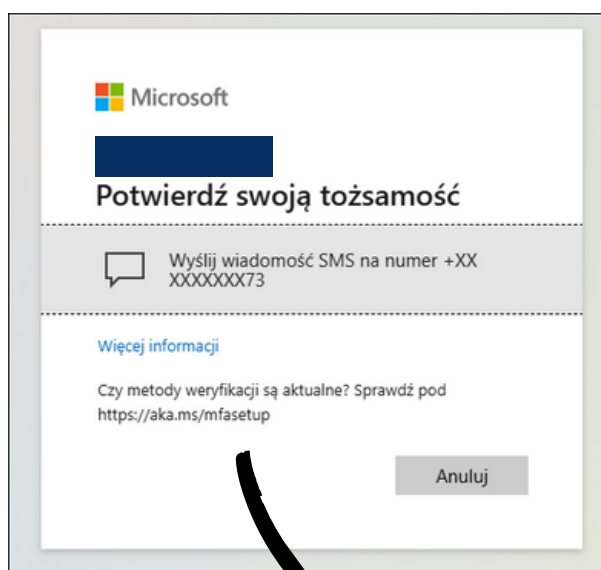
Konfiguracje przeprowadzamy tylko raz.

Od tego momentu, podczas logowania na konto i do wszystkich aplikacji Microsoft, uruchomione zostanie dodatkowe potwierdzenie w postaci kodu wysyłanego sms na podany numer telefonu.

Po wpisaniu adresu e-mail i hasła podczas logowania, pojawi się dodatkowe okno, w którym należy potwierdzić konieczność wysłania smsa.

Otrzymany kod należy wpisać w oknie przeglądarki.

Jeśli weryfikacja przebiegnie prawidłowo, proces logowania zostanie zakończony.

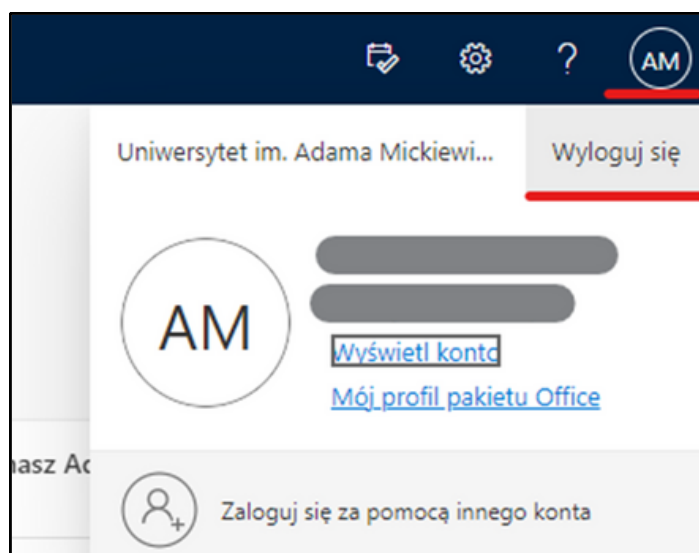


W celu zwiększenia bezpieczeństwa, zalecamy odznaczenie funkcji.

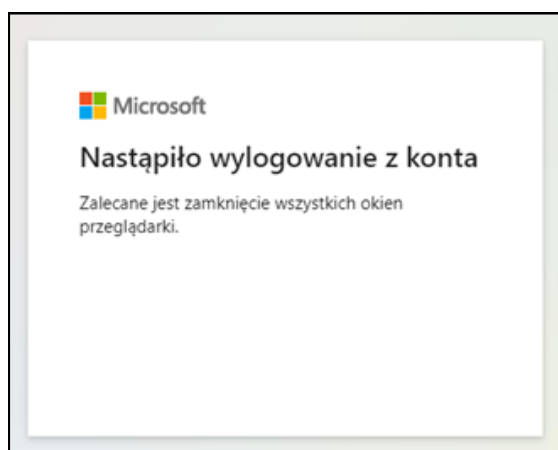


WYLOGOWANIE Z SYSTEMU

Jeśli chcemy się wylogować, należy w prawym górnym narożniku kliknąć na symbol osoby i z listy wybrać “Wyloguj się”.



Po chwili pojawi się komunikat o prawidłowym wylogowaniu.



Jeśli pojawią się problemy – prosimy kontaktować się z Wydziałowym Koordynatorem systemu USOS.

Aktualna lista Koordynatorów znajduje się na stronie [USOSweb](#).



Centrum Informatyczne UAM
helpdesk@amu.edu.pl
tel. 61 829 2670