Procedury dla użytkowników M365

Przygotowane przez:

Eryk Strzelecki, Ignacy Katkowski, Jacek Światowiak

APN Promise S.A.

2.0

Historia zmian w dokumencie

Data [RRRR-MM-DD]	Autor	Wersja	Opis zmian
2023-07-27	Eryk Strzelecki, Ignacy Katkowski	0.1	Utworzenie dokumentu, utworzenie procedur resetu haseł, konfiguracji MS Auth i logowania SMS
2023-07-31	Eryk Strzelecki	0.2	Aktualizacja dokumentu
2023-08-08	Eryk Strzelecki	0.3	Dodanie dodatkowych kroków, aktualizacja o dodatkowe ustawienia
2023-08-08	Jacek Światowiak	0.4	Aktualizacja krok przy wyborze jako domyślnego faktora Microsoft Authenticator i dodanie drugiego faktora - telefonu
2023-08-09	Adrianna Ostrowska	1.0	Przekazanie dokumentu do Zmawiającego
2023-08-24	Eryk Strzelecki	1.1	• Wyjaśnienie technicznych pojęć • Procedura logowania się do stacji • Opis innych składników uwierzytelniania • Instalacja aplikacji MS Auth
2023-08-25	Adrianna Ostrowska	2.0	Przekazanie dokumentu do Zmawiającego

Akceptacja dokumentu

Data [RRRR-MM-DD]	Osoba akceptująca	Zaakceptowana wersja	Podpis akceptującego

Wersjonowanie dokumentu

Numery wersji nadawane są w postaci: „0.1”, „1.1” dla roboczego statusu dokumentu. Dla zatwierdzonego formalnie dokumentu przyjęto numery wersji w formacie „1.0”.

Spis treści

1 Wstęp

Dokument zawiera opis procedur przeznaczonych dla użytkowników usług Microsoft 365, zawierające opis krok po kroku konfiguracji niektórych elementów na koncie oraz opis jak wykorzystać w praktyce poszczególne funkcjonalności.

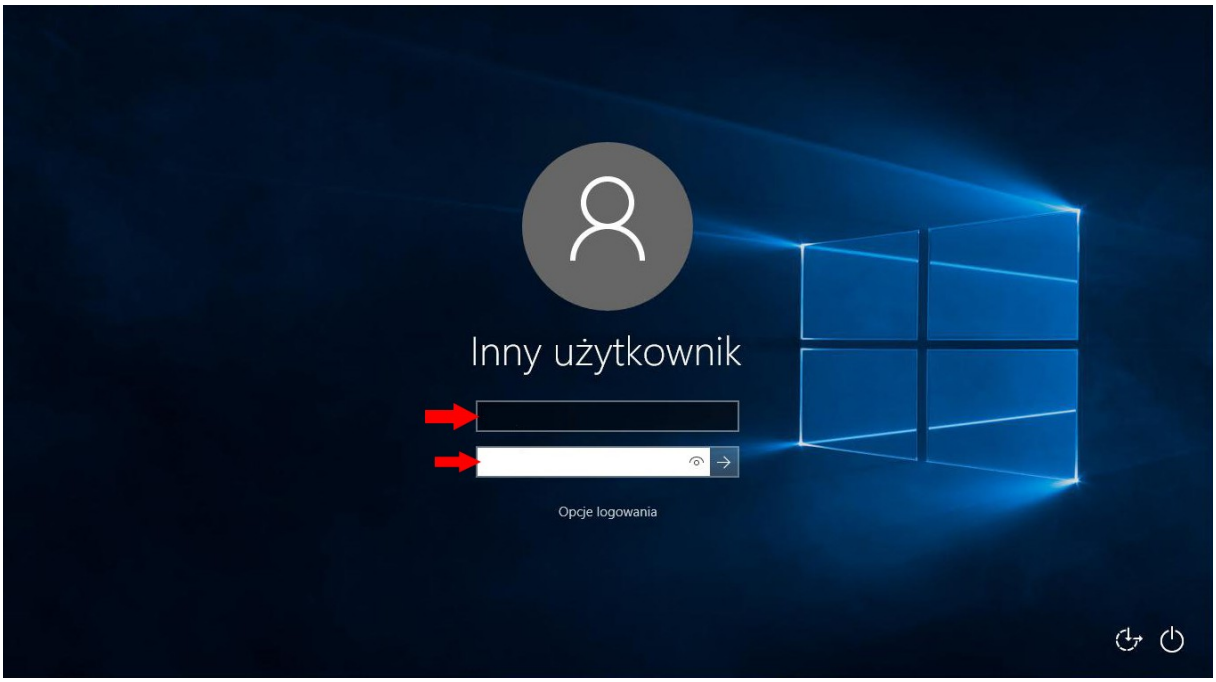
1.1 Wyjaśnienie pojęć

- **MFA –** (ang. Multi Factor Authentication) uwierzytelnianie wieloskładnikowe. Skrót ten najczęściej odnosi się do drugiego składnika uwierzytelniania (logowania się) do danego systemu, np. wymóg podania kodu SMS **po** uprzednim zalogowaniu się loginem i hasłem. Funkcja często wykorzystywana przy logowaniu do banku lub wykonywaniu płatności online, która zdecydowanie zwiększa bezpieczeństwo naszego konta.
- **Drugi składnik uwierzytelniania –** druga, wymagana metoda do zalogowania się na nasze konto. Pierwszym składnikiem jest zawsze nasze hasło, jednak jako drugi możemy wykorzystać:
  - Wiadomość SMS
  - Telefon wykonany przez automat na nasz numer telefonu
  - Wykorzystanie aplikacji służącej do obsługi MFA, np. Microsoft Authenticator
  - Wiadomość na wskazany adres e-mail
- **Microsoft Authenticator –** aplikacja firmy Microsoft na telefon. Pozwala na skonfigurowanie **MFA** w celu wykorzystania jej jako drugi składnik uwierzytelniania
- **SSPR –** opcja pozwalająca na samodzielny reset hasła przez stronę internetową, np. przy logowaniu się do aplikacji Microsoft przez przeglądarkę (strona portal.office.com). Po zmiane hasła tą metodą, hasło jest również zmieniane na naszym komputerze (przy następnym logowaniu do komputera, będziemy musieli podać nowe hasło)

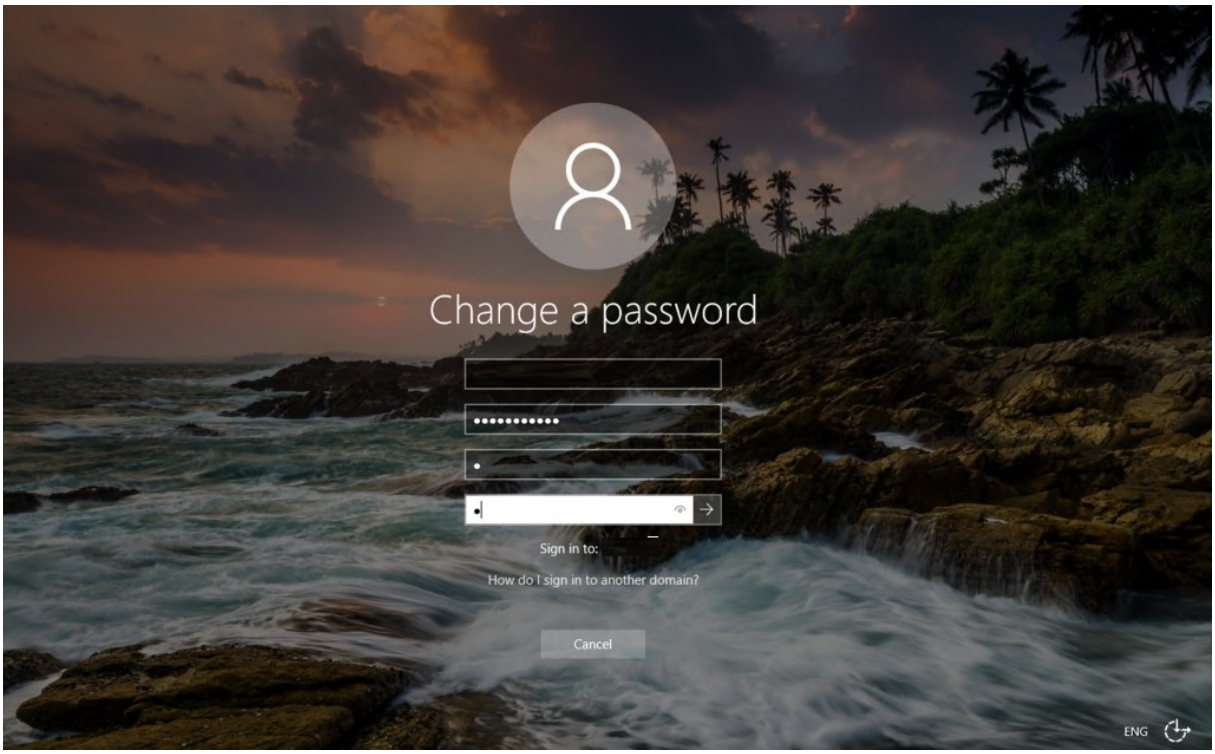
2 Procedura logowania się do stacji

Przy pierwszym logowaniu się do komputera, wymagane jest podanie loginu oraz hasła. Przy następnych logowaniach, jeżeli nikt inny nie logował się do komputera, nasze konto będzie automatycznie wyświetlane na górze ekranu zamiast informacji „Inny użytkownik".

W polach widocznych na rysunku poniżej, należy wprowadzić login oraz hasło do swojego konta.

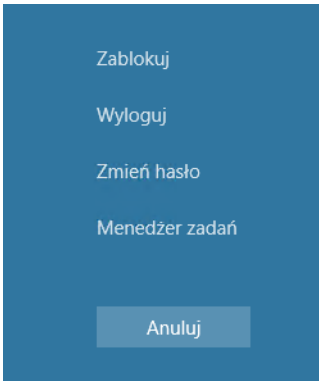


Przy pierwszym logowaniu, możliwe że zostaniemy poproszeni o zmianę hasła. Ekran ten może również pojawić się, jeżeli nasze poprzednie hasło straciło ważność i wymaga zmiany. W takiej sytuacji, należy podać kolejno: login i hasło (dane takie same jak na poprzednim ekranie) i wpisać dwa razy nowe hasło.



3 Procedura zmiany hasła

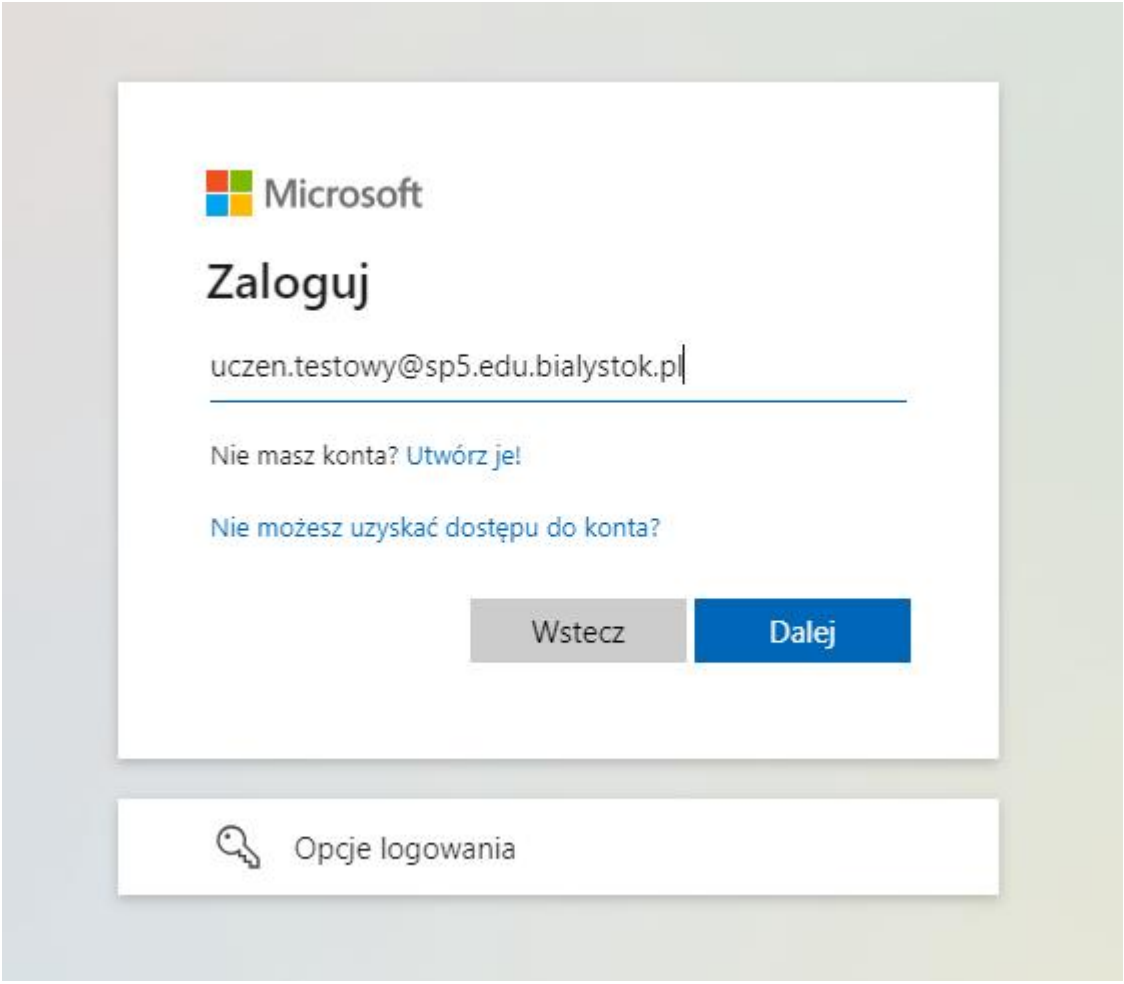
W poprzednim punkcie, przedstawiona została procedura logowania się do stacji wraz z wpisaniem nowego hasła. Jeżeli jednak chcemy sami zmienić hasło, możemy dokonać tego poprzez kliknięcie 3 przycisków jednocześnie (ctrl + alt + del) i wybranie opcji „Zmień hasło”.



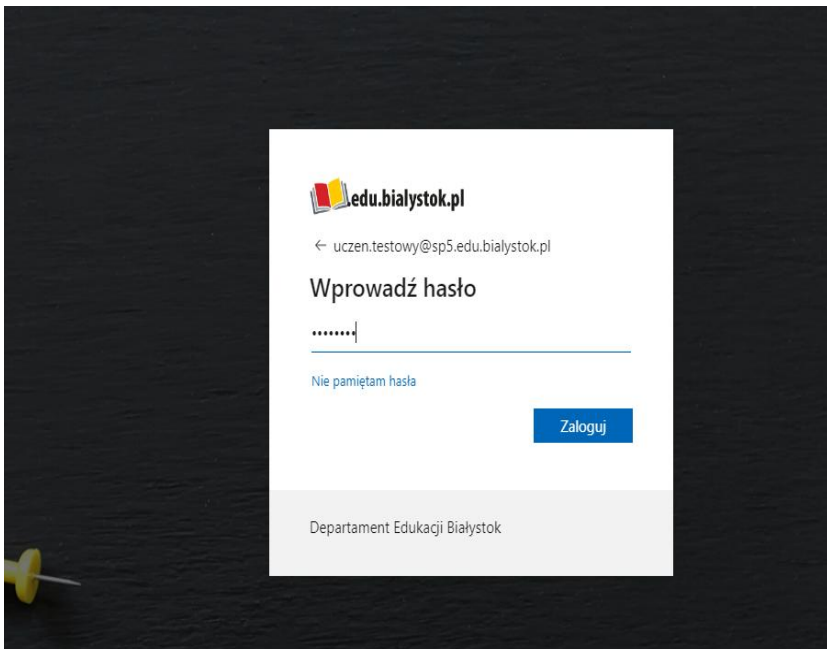
4 Procedura konfiguracji MFA

Niektóre kroki, zależnie od stanu konta i stanu konfiguracji MFA, mogą wyglądać inaczej, jednak zostało to zawarte przy odpowiednich punktach. Pierwsze logowanie do Microsoft 365 będzie wymagało skonfigurowania MFA, zgodnie z tą procedurą.

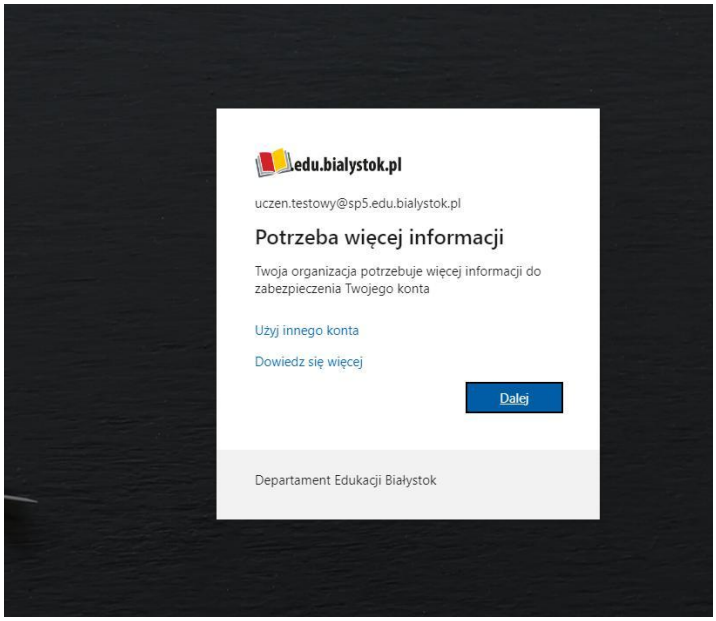
1. W przeglądarce przejdź na główną stronę logowania Microsoft 365, która jest dostępna pod adresem portal.office.com. Wyświetlony zostanie ekran logowania w który należy wpisać swój adres e-mail.



2. Na następnym ekranie, należy wpisać hasło (takie samo jak do komputera).

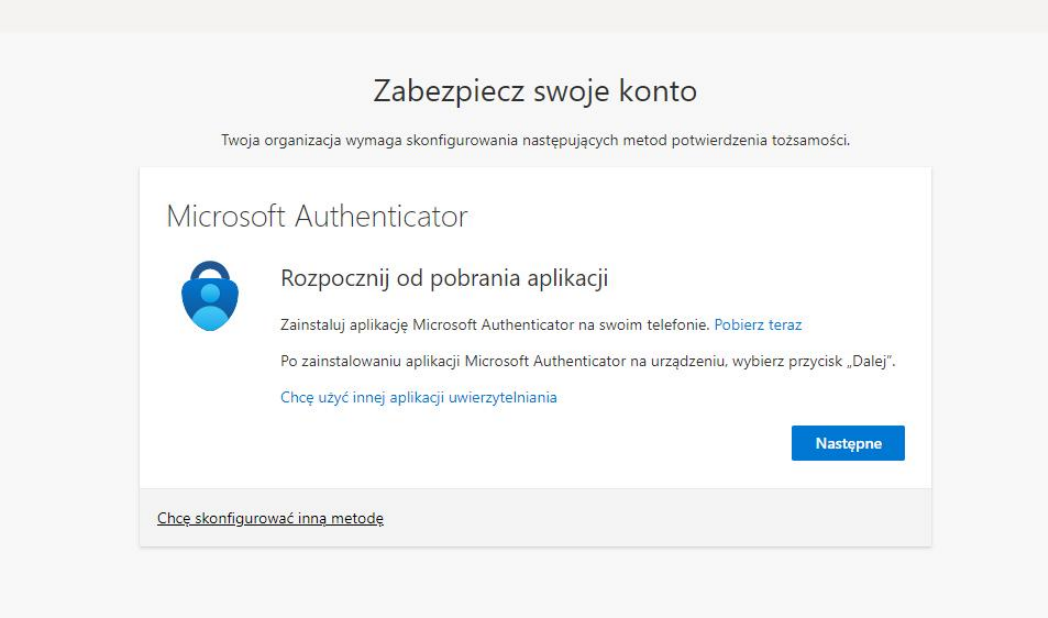


3. Przy pierwszym logowaniu, po wprowadzeniu loginu i hasła, otrzymamy komunikat informujący o potrzebie podania dodatkowych informacji.

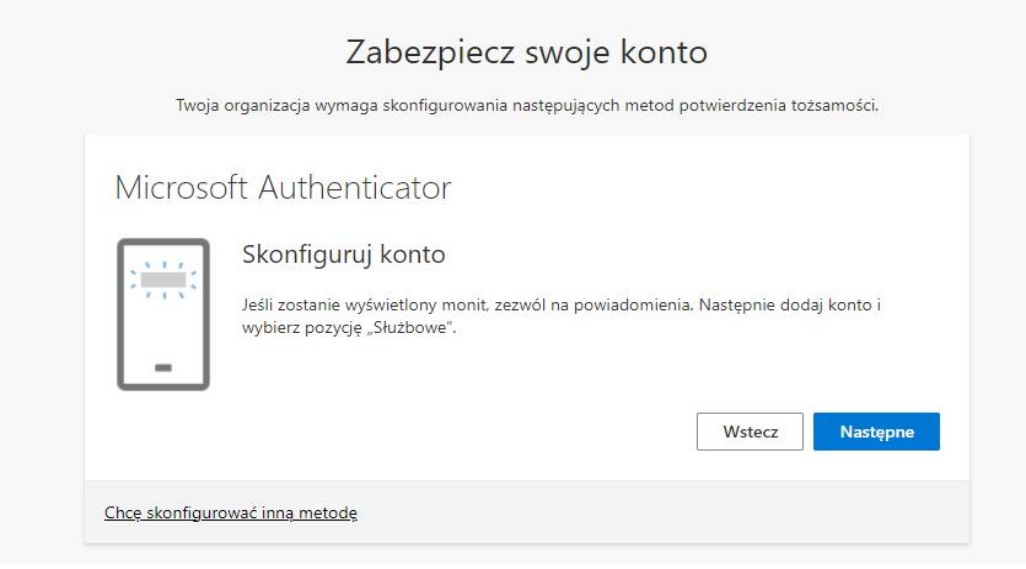


3.1. W konfiguracji domyślnej – konfigurujemy metodę uwierzytelnienia dwuskładnikowego Microsoft Authenticator (MFA). Jednak jeżeli chcemy wykorzystać inną metodę uwierzytelnienia, musimy użyć przycisku „Chcę skonfigurować inną

metodę" i wybrać zamiast aplikacji Microsoft Authenticator np. wiadomość SMS (metodę opisano w pkt. 4.1 Wykorzystanie innego drugiego składnika).



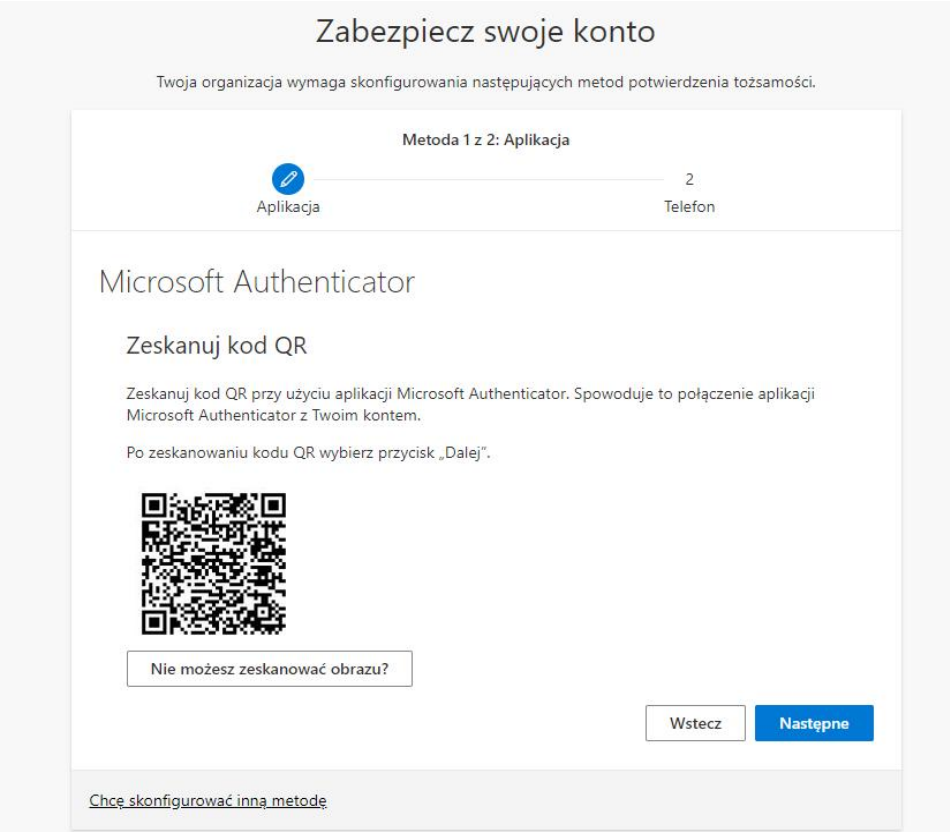
4. Klikamy przycisk „Następne"



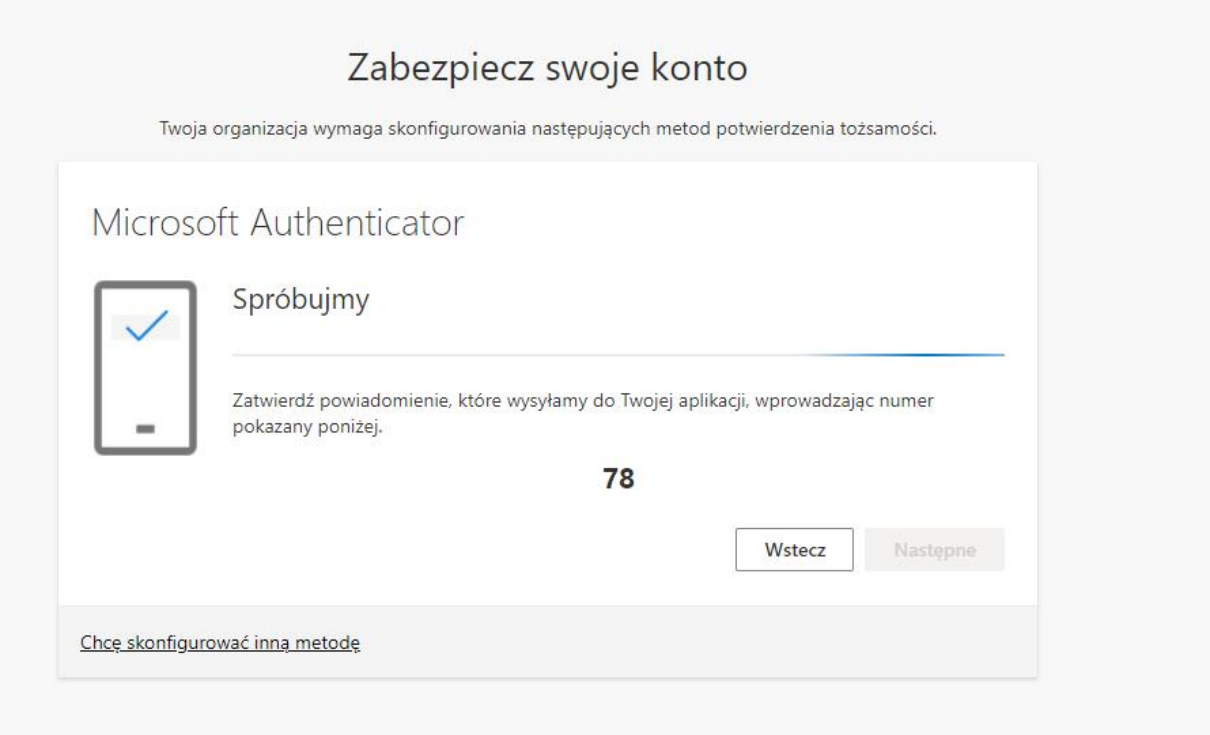
5. Pobieramy i instalujemy na telefonie, który będzie wykorzystywany w procesie uwierzytelniania aplikację **Microsoft Authenticator** (sposób pobrania aplikacji w zależności od rodzaju telefonu opisano w pkt. 8 Instalacja aplikacji Microsoft Authenticator).

   W aplikacji wyświetlona zostanie instrukcja z opisem krok po kroku, jak skonfigurować

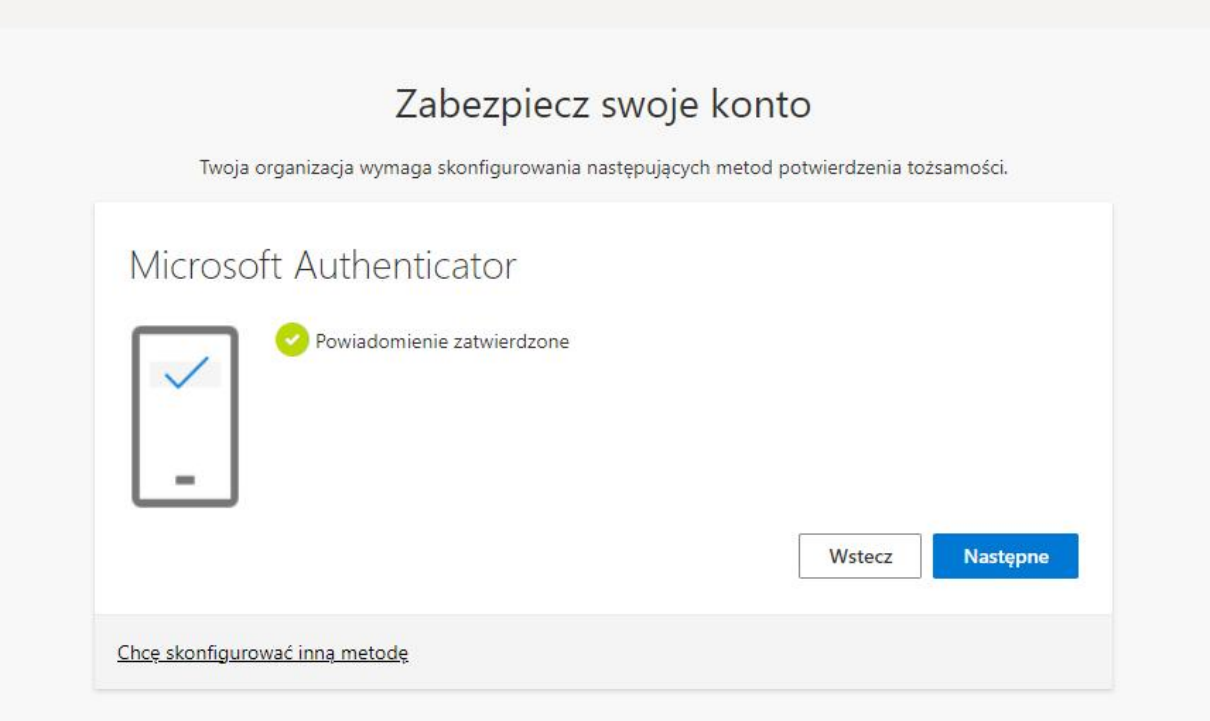
swoje konto, jeżeli jednak to nie nastąpi, należy kliknąć przycisk ikonę **+ ,** następnie wybrać **Konto służbowe,** a potem w oknie **Dodaj konto służbowe** opcję **Zeskanuj kod QR.**



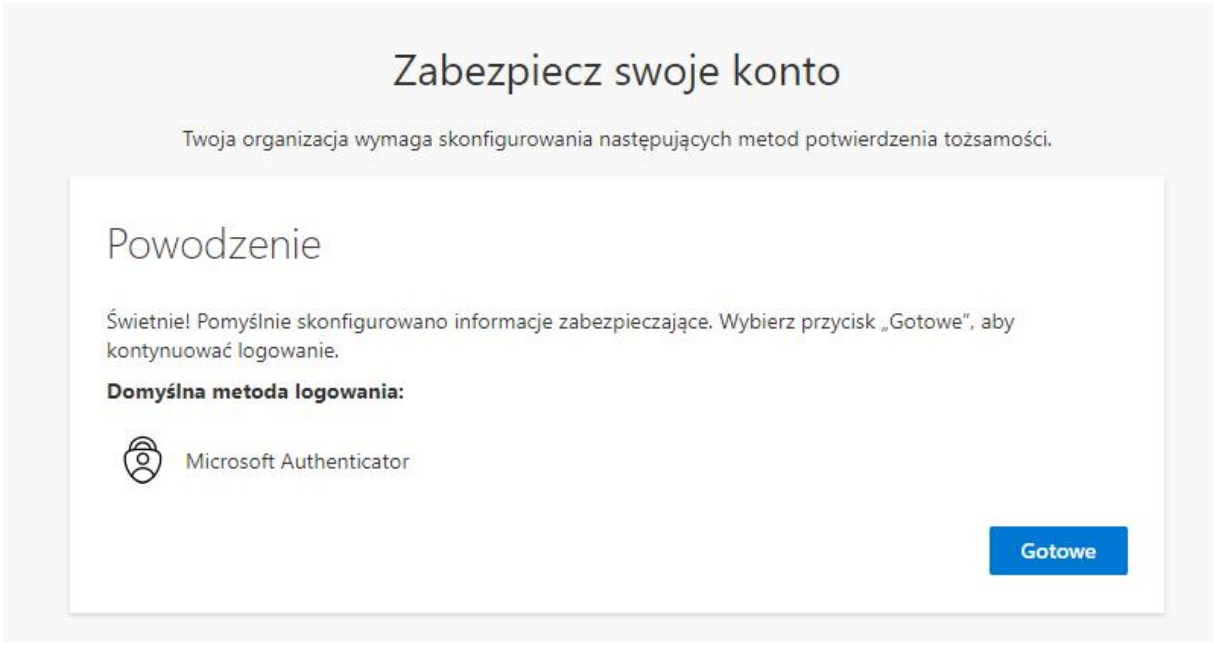
6. Należy zeskanować przy pomocy telefonu widoczny na ekranie kod QR i potwierdzić logowanie za pomocą wpisania dwucyfrowej liczby widocznej na ekranie.



7. Klikamy przycisk „Następne”



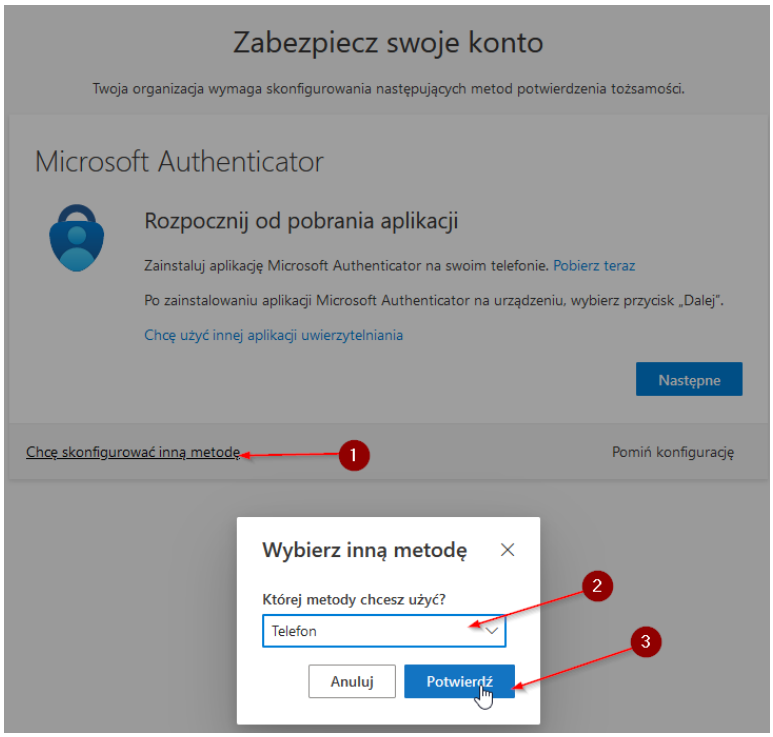
8. Klikamy przycisk „Gotowe”


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:
Microsoft Authenticator
Gotowe

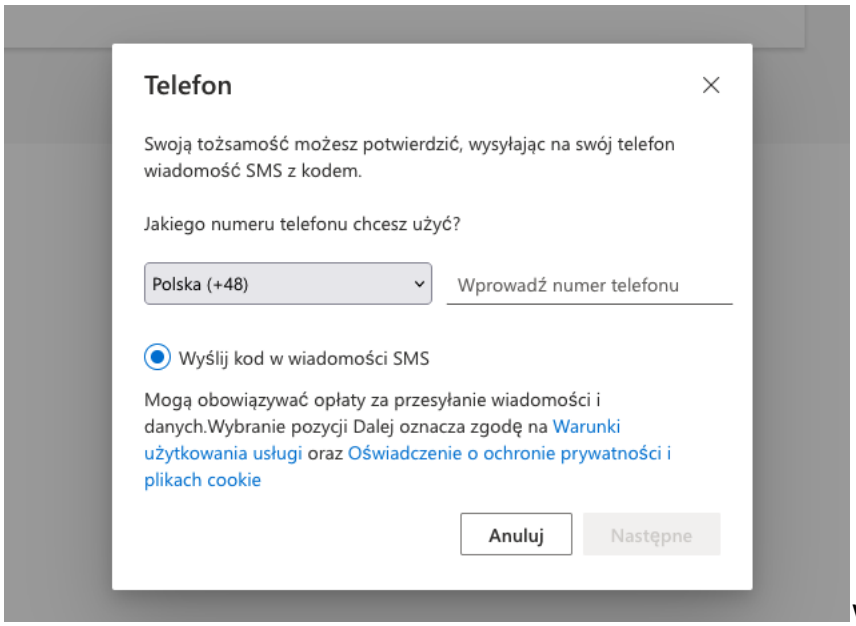
9. Dopiero teraz, po przejściu kroków konfiguracji MFA, pojawia się okno o zmianę naszego hasła.

4.1 Wykorzystanie innego drugiego składnika

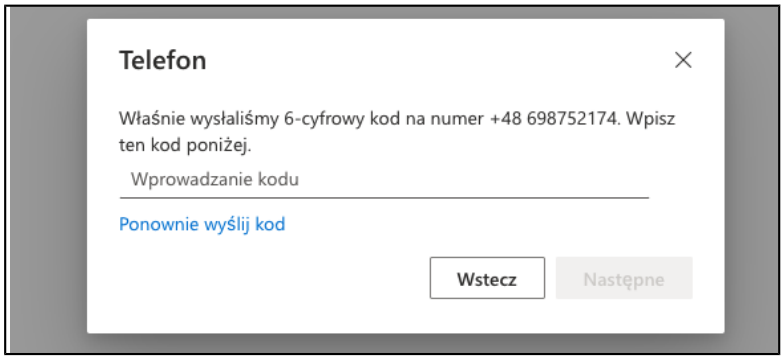
1. Jeżeli nie planujemy wykorzystywać bezpośrednio aplikacji **Microsoft Authenticator** wówczas należy wybrać opcję „Chcę skonfigurować inną metodę”, a następnie wybrać z listy rozwijanej „Telefon” i przejść dalej.



2. Następnie z listy rozwijanej wybieramy numer kierunkowy do Polski (+48) i wprowadzamy nasz numer telefonu:

3. 

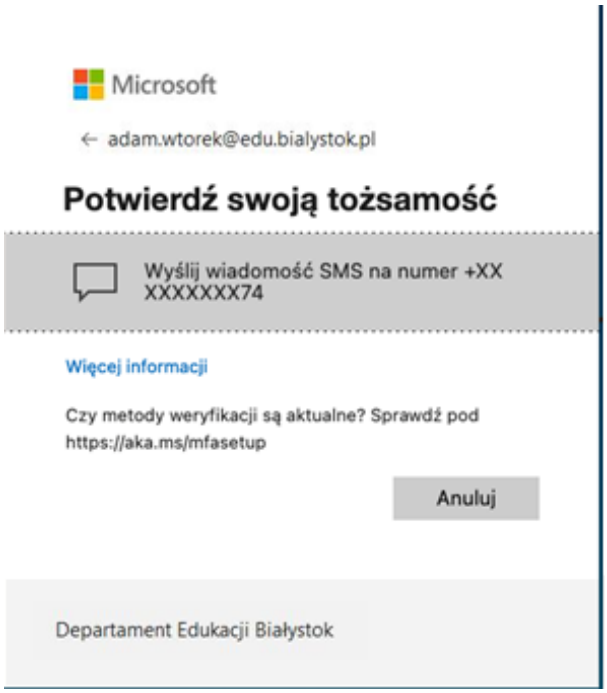
W następnym oknie, należy wpisać 6-cyfrowy kod, który otrzymamy SMS-em na podany numer:



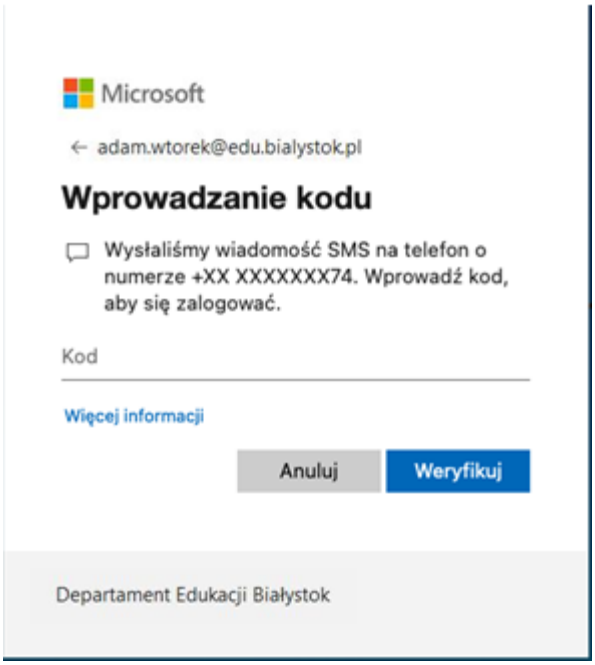
Klikamy „Następne”

4. Weryfikacja przeszła prawidłowo, telefon został pomyślnie zarejestrowany:

5. Teraz przy logowaniu będziemy musieli podać kod SMS. Klikamy „Wyślij wiadomość SMS na numer +XX…”

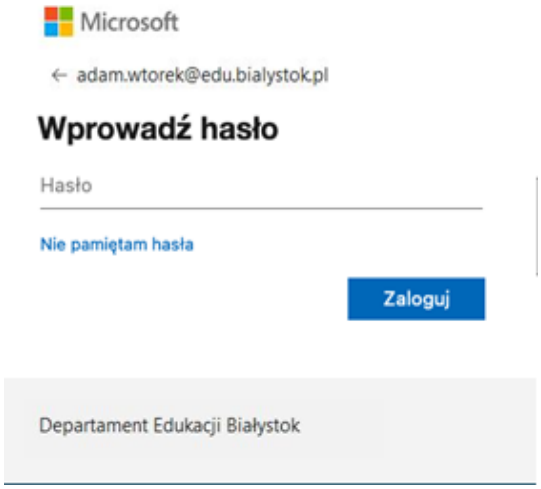


6. Wpisujemy kod, który otrzymaliśmy SMS-em i po wpisaniu, klikamy „Weryfikuj”– jesteśmy zalogowani.



5 Procedura resetu hasła – SSPR

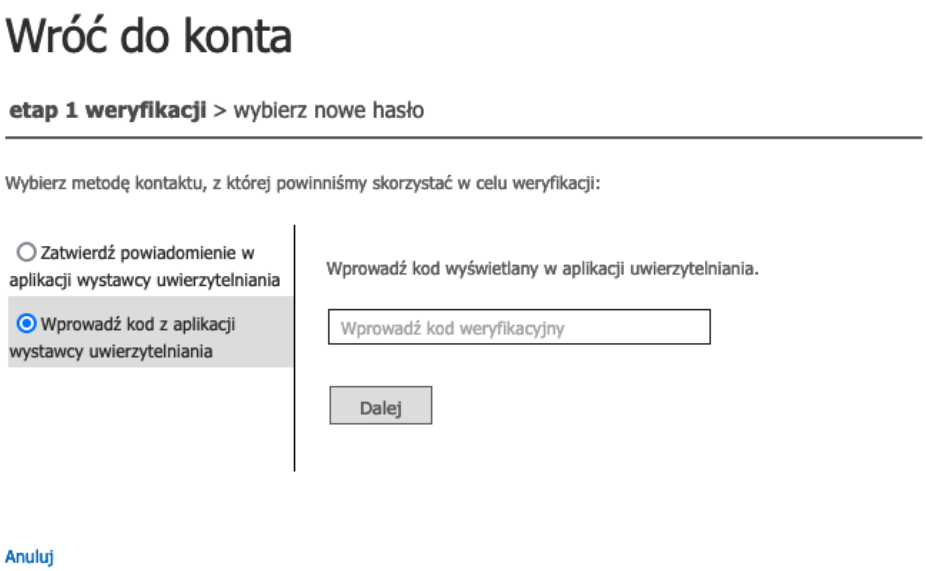
1. W oknie wpisywania hasła na stronie portal.office.com, klikamy „Nie pamiętam hasła”:



2. Wpisujemy nasz adres e-mail i przepisujemy kod Captcha (litery z obrazka):

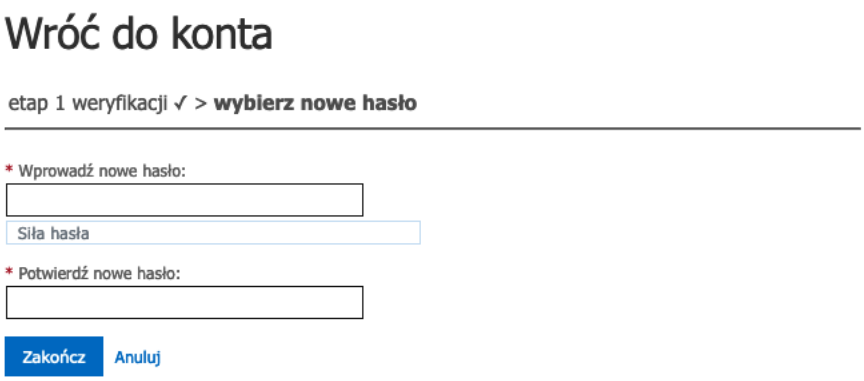
Klikamy „Dalej

3. Wybieramy jedną z dostępnych metod resetu hasła po lewej stronie. Jeżeli do weryfikacji wybraliśmy wcześniej aplikację Microsoft Authenticator , zaznaczamy opcję wyboru „Wprowadź kod z aplikacji wystawcy uwierzytelniania”.
   W przypadku wybrania innej metody uwierzytelniania np. SMS-a, będziemy mogli wybrać nasz numer telefonu.

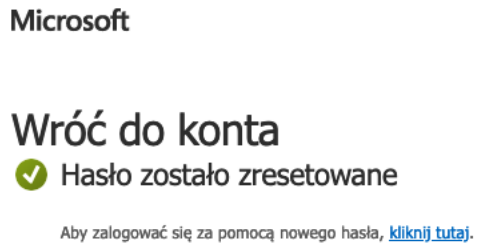


   Po uzupełnieniu danych, klikamy „Dalej”

4. Wpisujemy nowe hasło:



5. Hasło zostało zmienione, możemy logować się za pomocą nowych poświadczeń:

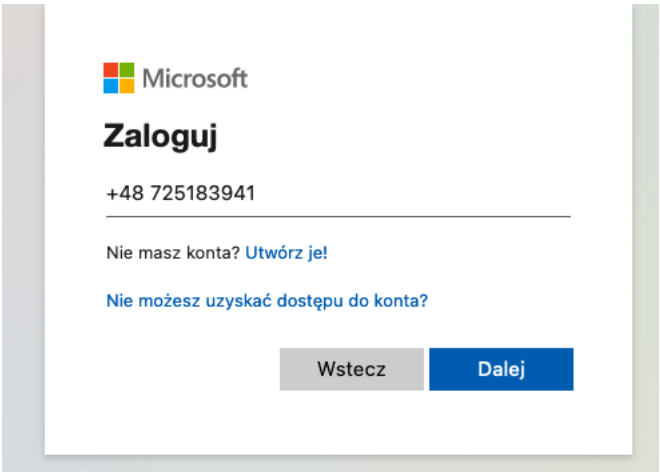


Uwaga - ze względu na synchronizację zmiany haseł, należy odczekać około 2 minuty, zanim będziemy mogli zalogować się do aplikacji i komputera za pomocą nowego hasła

6 Procedura logowania za pomocą hasła na SMS

Ten typ logowania zadziała dopiero po pierwszym zwykłym logowaniu na swoje konto (za pomocą adresu e-mail i hasła) i skonfigurowaniu numeru telefonu lub aplikacji jako drugi składnik uwierzytelniania.

1. W oknie logowania wpisujemy nasz numer telefonu

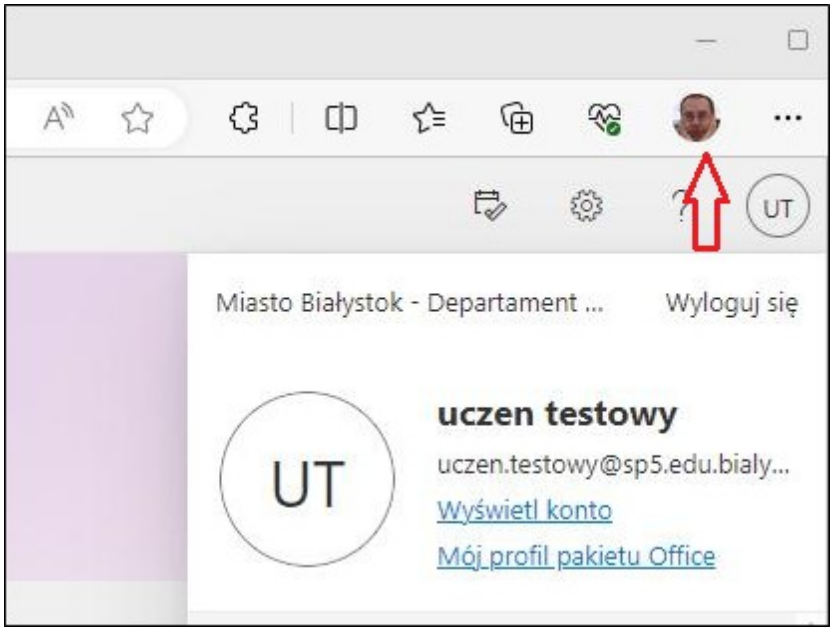


2. Po wybraniu przycisku **Dalej** zostaniemy poproszeni o wpisanie kodu, który otrzymamy SMS-em
3. Wpisujemy kod, a następnie jesteśmy zalogowani.

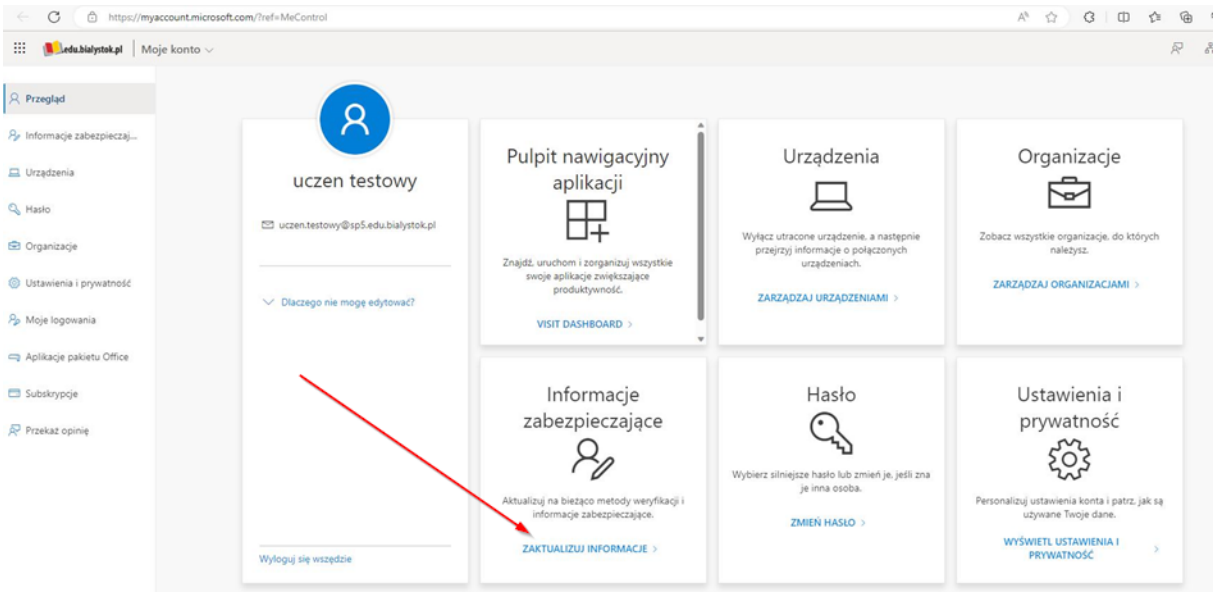
7 Procedura dodania innego składnika uwierzytelniania lub numeru telefonicznego

Jeżeli planujemy wykorzystać inny składnik do procesu uwierzytelniania np. skonfigurowaliśmy aplikację Microsoft Authenticator i chcemy teraz skonfigurować dodatkowo SMS, należy dodać numer telefonu komórkowego do naszego konta.

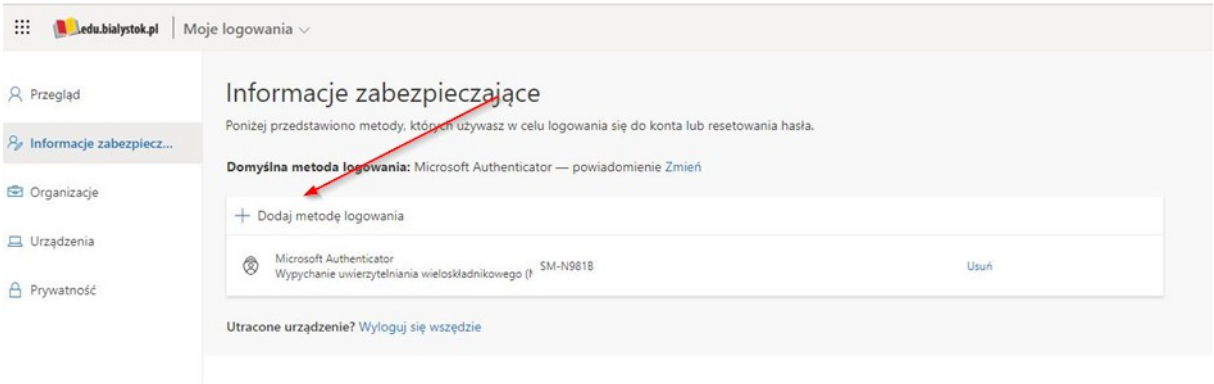
1. Po zalogowaniu się na portal.office.com, na głównym widoku klikamy na ikonę użytkownika z naszymi inicjałami lub zdjęciem w prawy, górnym rogu przeglądarki i wybieramy **Wyświetl konto**



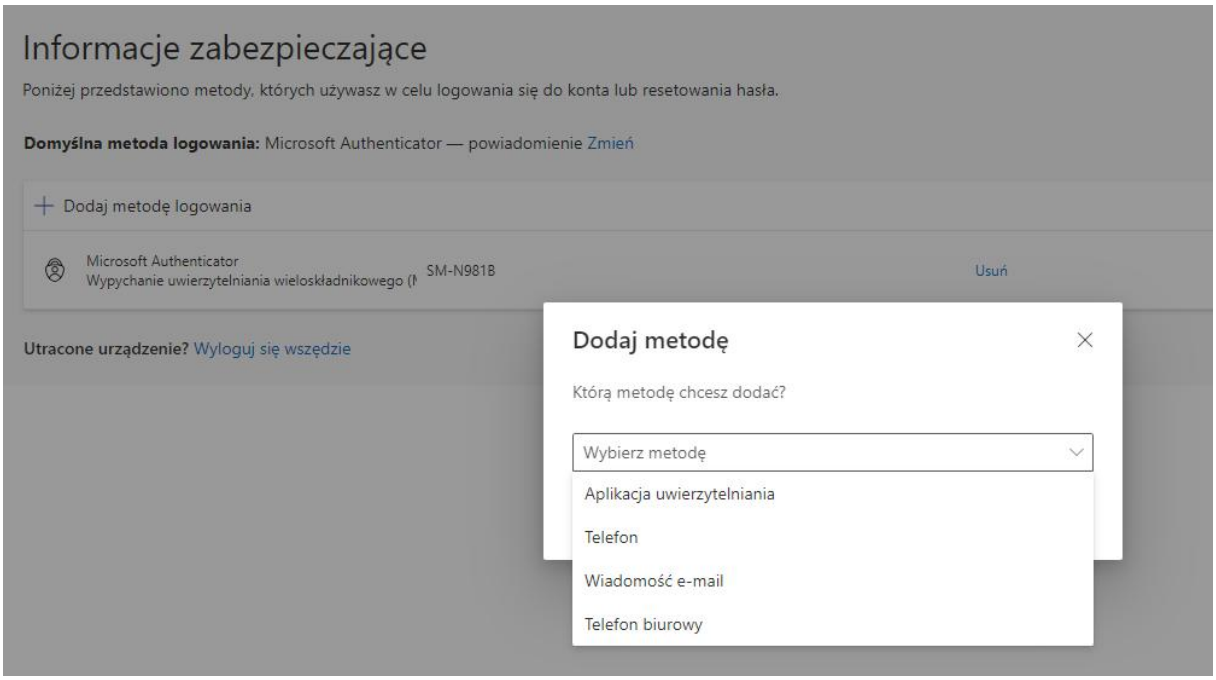
2. Klikamy w kafelek – **Informacje zabezpieczające**



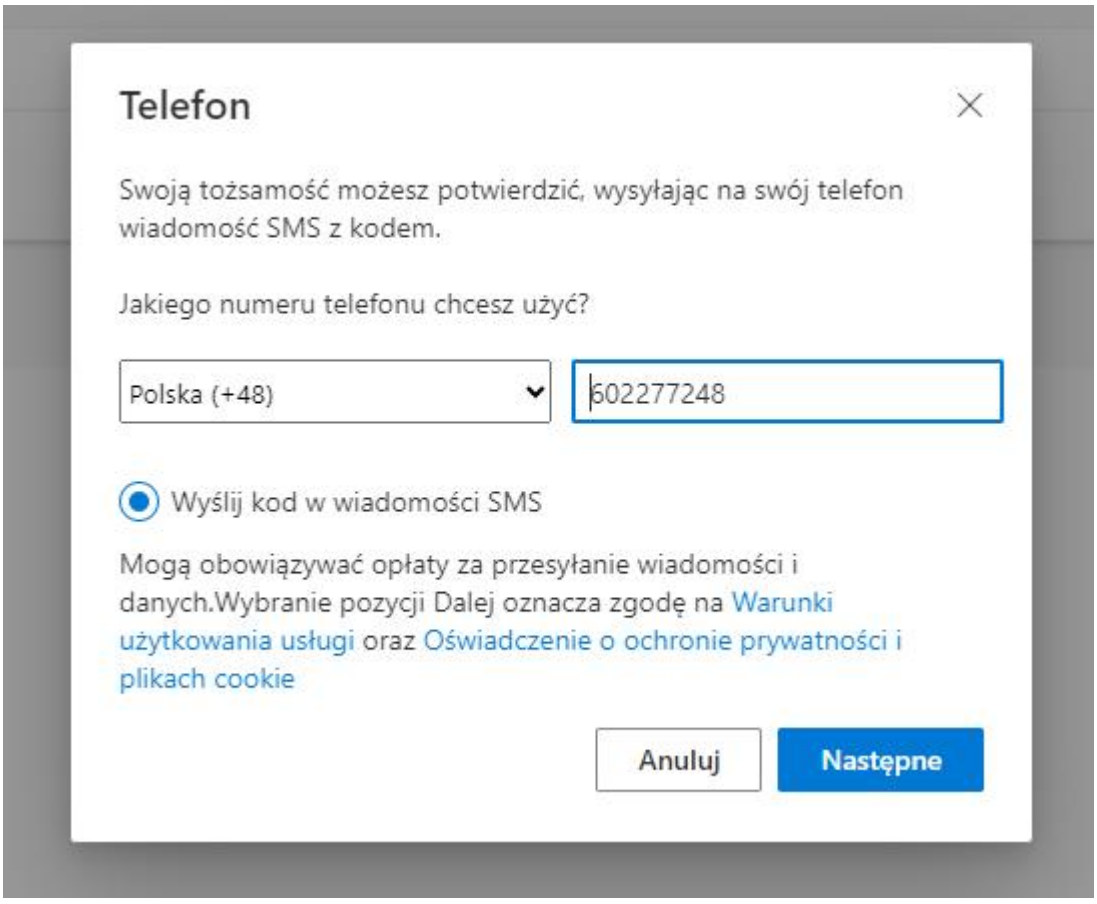
3. W nowym oknie klikamy w ikonę **+ Dodaj metodę uwierzytelniania**



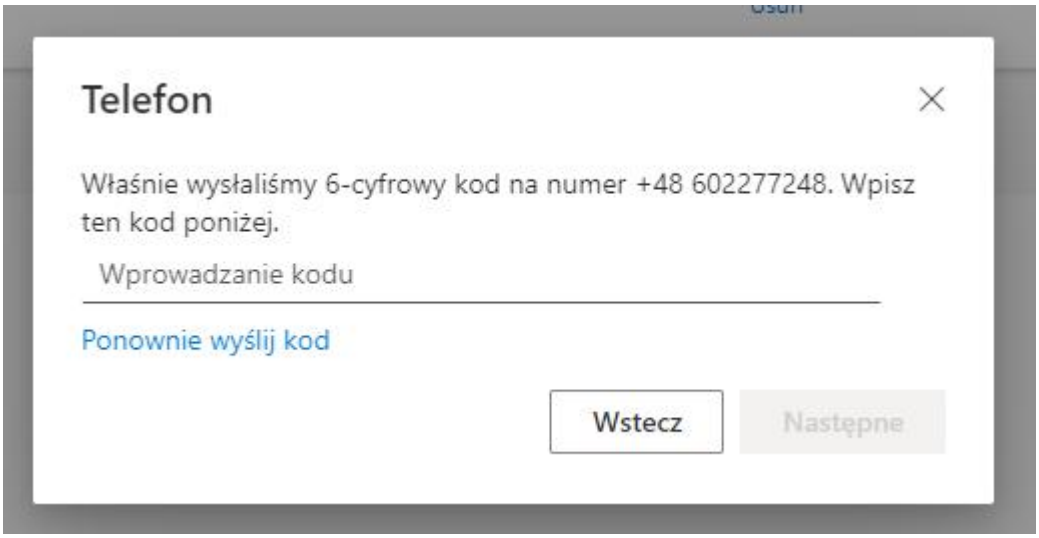
4. Następnie z listy metod uwierzytelniania wybieramy Telefon



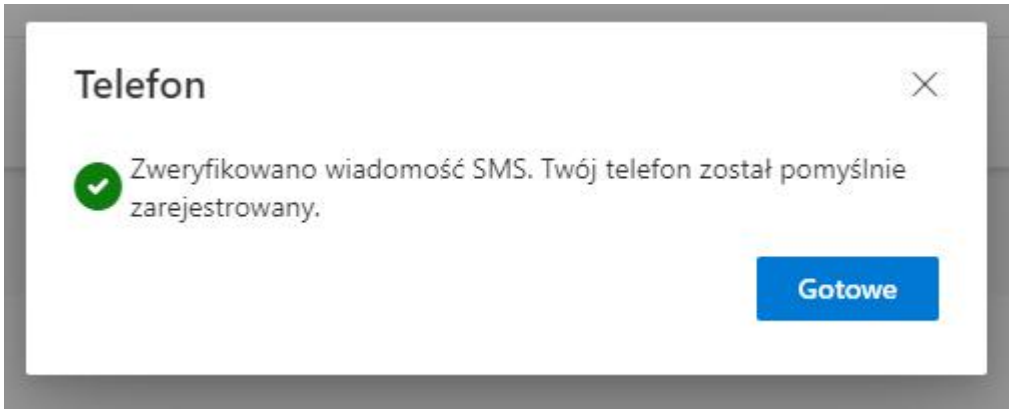
5. Wybieramy kraj Polska i podajemy 9 cyfrowy numer telefonu



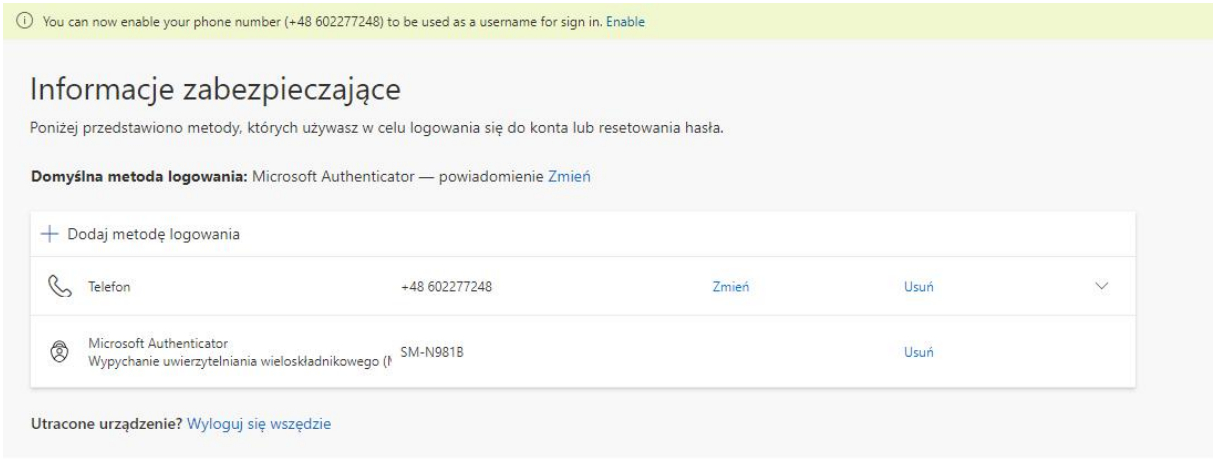
6. Na telefon przyjdzie SMS z kodem jednorazowym – wprowadzamy go w oknie jak poniżej.



7. Po poprawnej weryfikacji – telefon zostaje dodany.



8. Teraz na liście mamy dostępne dwa drugie składniki uwierzytelniania
   8.1. Microsoft Authenticator
   8.2. Telefon (czyli jednorazowy SMS)

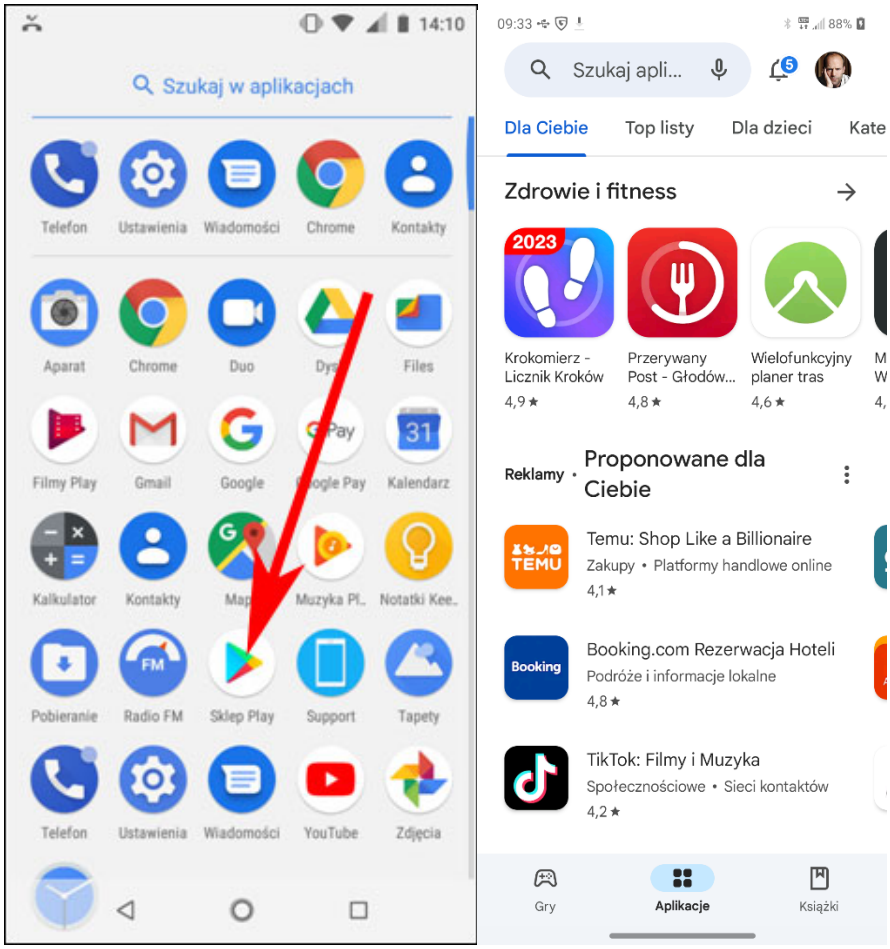


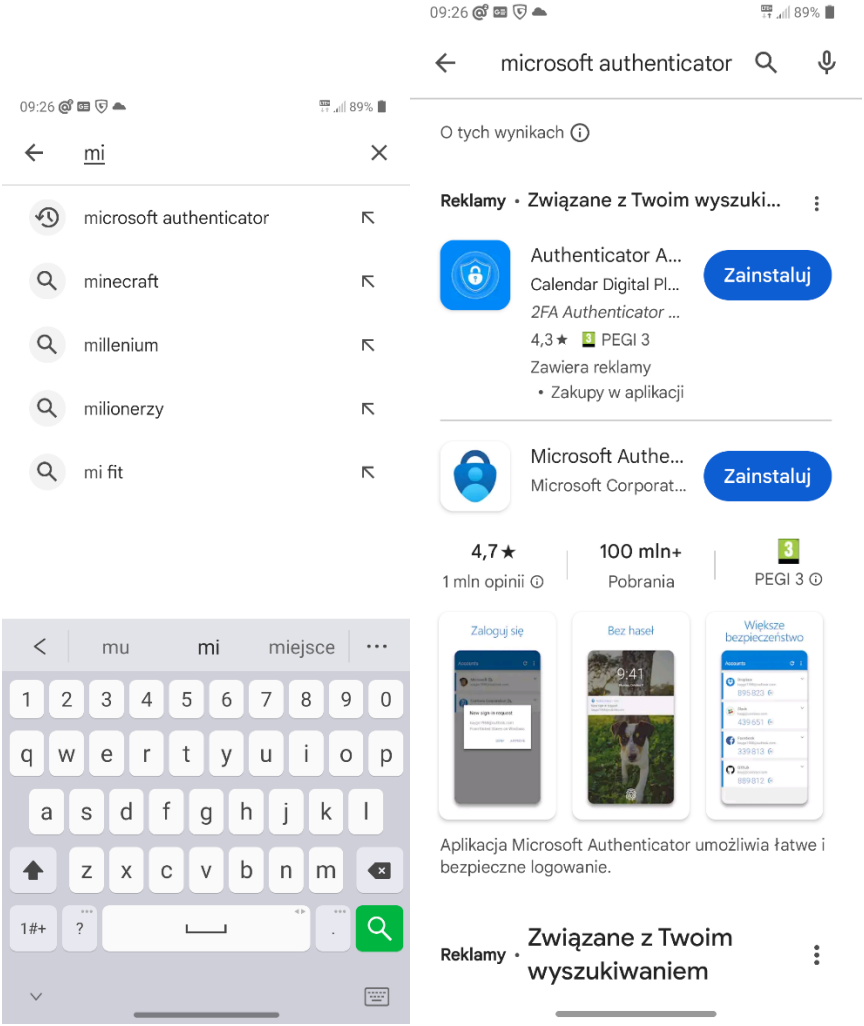
8 Instalacja aplikacji Microsoft Authenticator

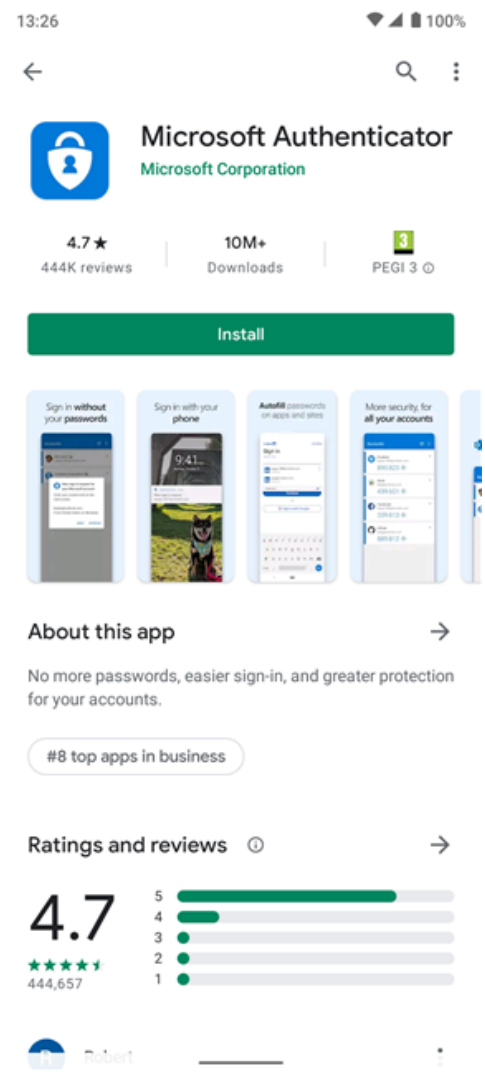
W przypadku chęci wykorzystania aplikacji Microsoft Authenticator do uwierzytelniania za pomocą MFA, należy pobrać aplikację ze sklepu dostępnego na telefonie. Wygląd może różnić się w zależności od systemu na telefonie, jednak poniżej przedstawione zostały miejsca, skąd ją pobrać na różnych telefonach.

8.1 Android

Na telefonie z systemem android, należy odnaleźć aplikację **Sklep Play**, w której należy wyszukać aplikację **Microsoft Authenticator** i ją zainstalować.




09:26
89%
mi
microsoft authenticator
minecraft
millenium
milionerzy
mi fit
mu
mi
miejsce
1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
1#+
?
09:26
89%
microsoft authenticator
O tych wynikach
Reklamy • Związane z Twoim wyszuki...
Authenticator A...
Calendar Digital Pl...
2FA Authenticator ...
4,3★ PEGI 3
Zawiera reklamy
• Zakupy w aplikacji
Zainstaluj
Microsoft Authe...
Microsoft Corporat...
Zainstaluj
4,7★
1 mln opinii
100 mln+
Pobrania
PEGI 3
Zaloguj się
Bez haseł
Większe bezpieczeństwo
Aplikacja Microsoft Authenticator umożliwia łatwe i bezpieczne logowanie.
Reklamy • Związane z Twoim wyszukiwaniem


13:26
100%
Microsoft Authenticator
Microsoft Corporation
4.7★
444K reviews
10M+
Downloads
PEGI 3
Install
About this app
No more passwords, easier sign-in, and greater protection for your accounts.
#8 top apps in business
Ratings and reviews
4.7
444,657
5
4
3
2
1

8.2 iOS/iPhone

W przypadku telefonów z systemem iOS (iPhone) należy otworzyć **App Store** i tak samo jak w przypadku systemu Android, wyszukać aplikację **Microsoft Authenticator** i ją zainstalować.

8.3 Huawei

W przypadku telefonów marki Huawei, aplikacji **Microsoft Authenticator** należy szukać w **AppGallery.**