

Dwuetapowa weryfikacja – czyli co musisz o niej wiedzieć

Weryfikacja 2FA (zwana dwuetapową) jest dzisiaj niezwykle ważna, gdyż coraz częściej dochodzi do wycieków danych.

Dlatego zalecamy włączenie Ci tej opcji, wtedy masz pewność, że nic Ci się nie stanie z kontem społecznościowym.

Tym bardziej, że samo mocne hasło nie uchroni nas przed włamaniami na różne konta np. społecznościowe.

Co to jest weryfikacja dwuetapowa?

Weryfikacja dwuetapowa (nazywana też uwierzytelnianiem dwuskładnikowym) zapewnia dodatkowy poziom bezpieczeństwa konta w razie utraty hasła.

Po jej skonfigurowaniu możesz logować się na swoje konto za pomocą: hasła, telefonu.

Jak działa technologia i dlaczego 2FA jest ważne?

- 2FA zabezpiecza proces logowania, które są najczęściej wymierzone w słabe hasła bądź w skradzione dane,
- Pomaga również przy tym, jeśli osoba zna twoje dane do logowania, to musi mieć dostęp za pomocą kodu,

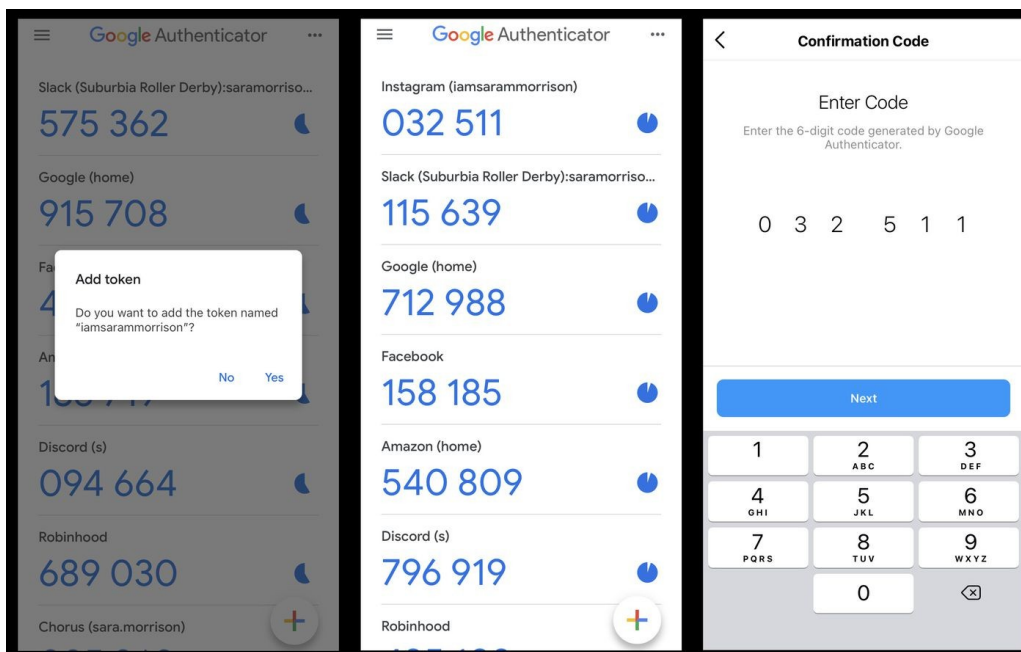
- Uwierzytelnianie dwuskładnikowe jest skutecznym sposobem przed tego typu atakami jak: phishing, social engineering oraz atakami na hasła typu brute force,

Uwierzytelnienie dwuskładnikowe jest bardzo ważne, ponieważ metody hakerów są cały czas opracowywane, niestety im te próby wychodzą, dlatego też został opracowany nowy mechanizm jak 2FA utrudniający nieuprawnionym dojście do naszych kont.

Przykłady aplikacji do uwierzytelniania dwuskładnikowego:

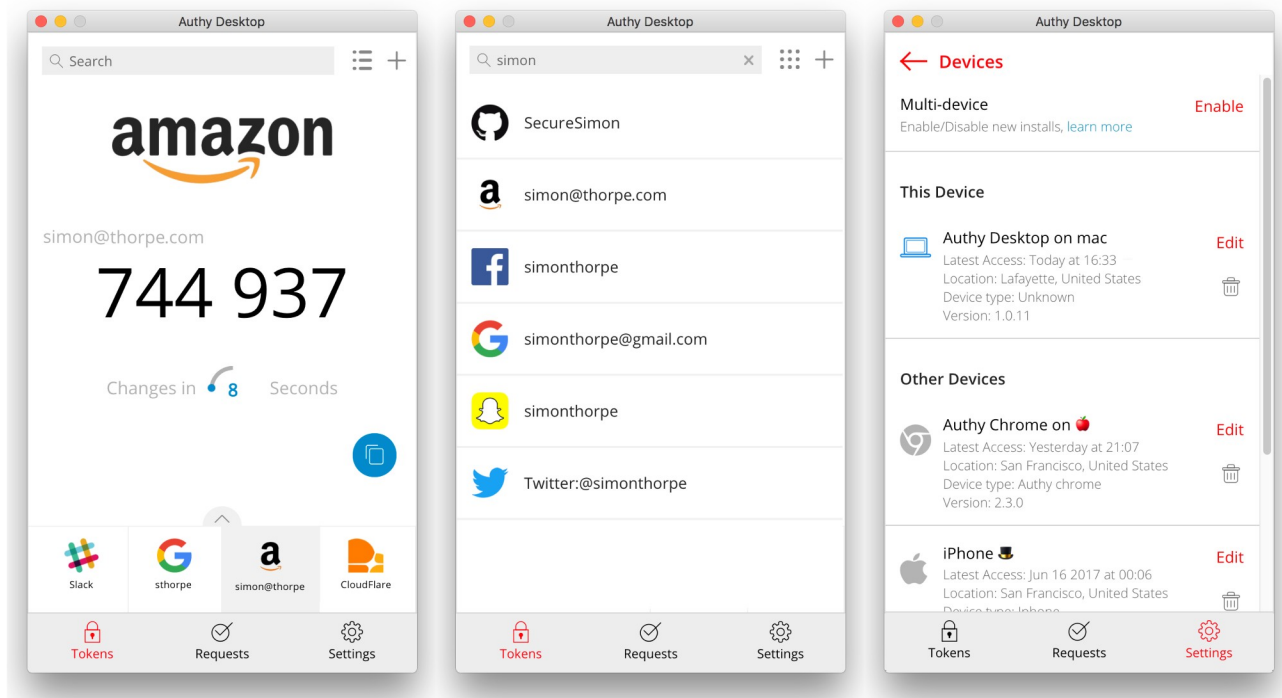
Jest wiele programów, które ułatwiają nam zabezpieczenie kont. Tu przedstawię Ci te najpopularniejsze i zarazem najlepsze.

- Google Authenticator



To najchętniej wybierana aplikacja mobilna do logowania dwuetapowego. Po jej sparowaniu z danym kontem program generuje sześć cyfr, które są konieczne do podania podczas uwierzytelniania dwuskładnikowego.

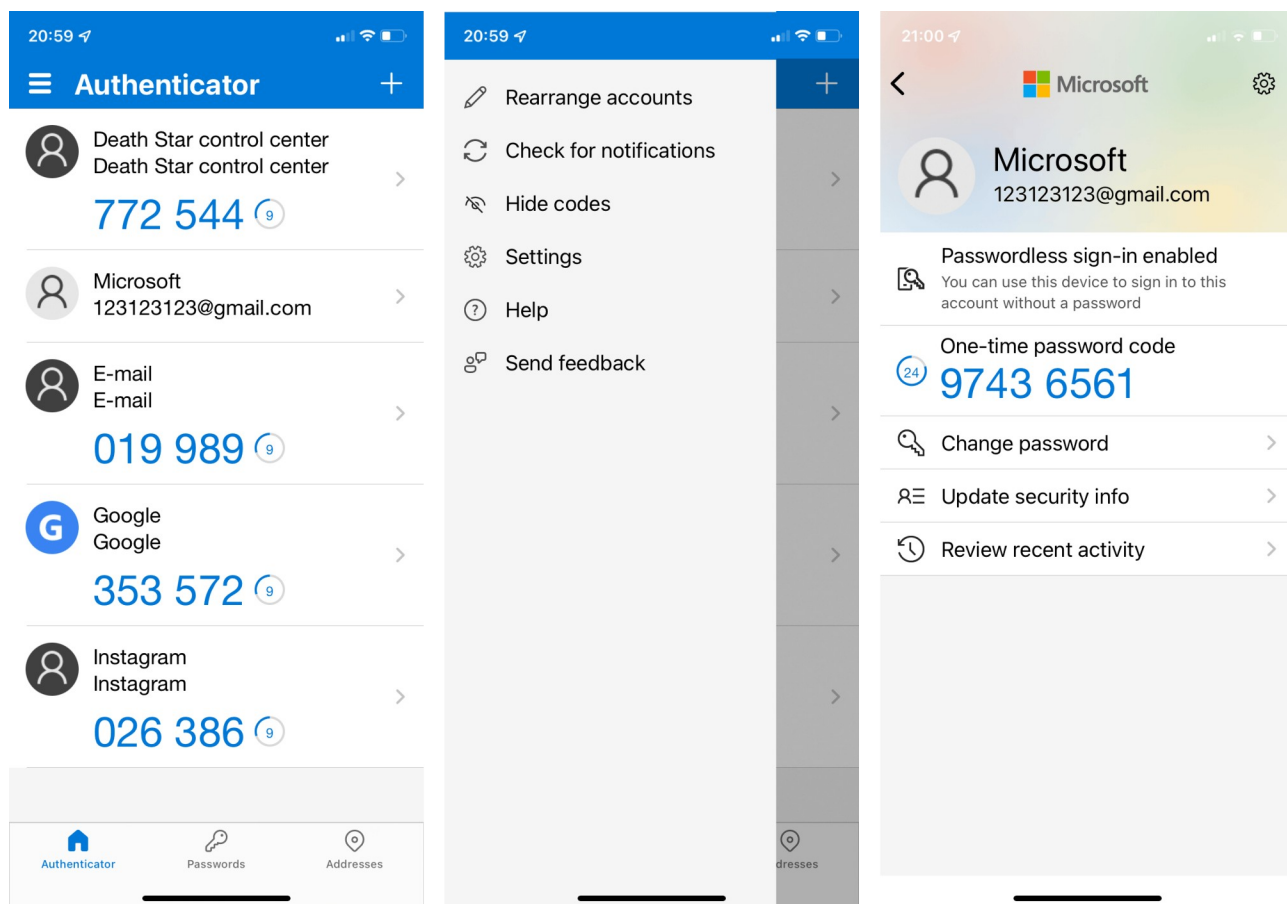
- Authy



Kolejna bardzo podobna aplikacja, czyli wyżej wspomniana „Google Authenticator”. Ten program charakteryzuje to, że nawet laik poradzi sobie z obsługą takiego narzędzia.

Działa również tak samo jak wyżej wspomniana aplikacja, czyli generuje cyfry lub kod QR podawane przy logowaniu dwuskładnikowym.

- Microsoft Authenticator



Aplikacja ta zaś umożliwia logowanie się do osobistego konta Microsoft bez konieczności podawania hasła – a także generowanie kodów dla innych serwisów.

Jak to działa? Pierwsza opcja autoryzuje Twoją tożsamość za pomocą Face ID bądź odcisku palca.

Jeśli zgubisz smartfona, a chcesz zalogować się na nowym urządzeniu, wystarczy podać kod PIN.

W tym przypadku program wysyła jednorazowy kod do sparowania na innym koncie niż Microsoft.