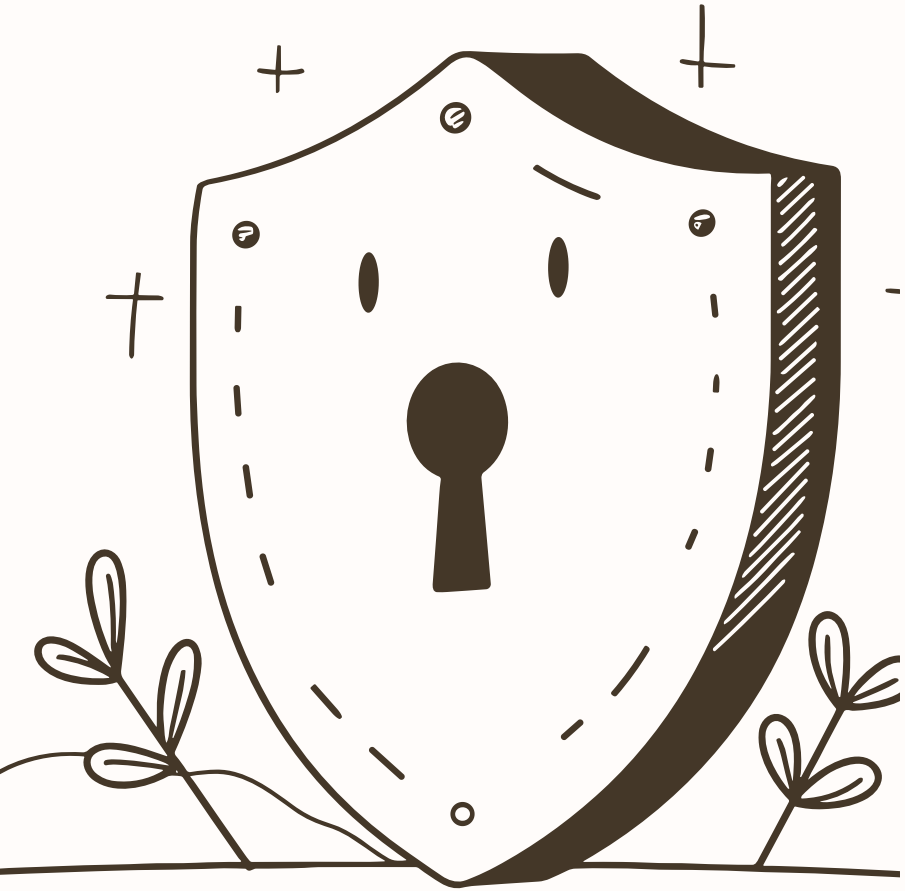


Uwierzytelnianie dwuskładnikowe (2FA) - skuteczna ochrona kont

Uwierzytelnianie dwuskładnikowe (2FA) to nowoczesne rozwiązanie, które znacząco zwiększa bezpieczeństwo Twoich kont internetowych. Dzięki 2FA możesz skutecznie zabezpieczyć swoje dane osobowe, finansowe i służbowe przed cyberprzestępcami.

W tej prezentacji dowiesz się, czym jest uwierzytelnianie dwuskładnikowe, jak działa oraz dlaczego warto je stosować w codziennym korzystaniu z internetu.

Co to jest uwierzytelnianie dwuskładnikowe?

Definicja

Uwierzytelnianie dwuskładnikowe (ang. Two-Factor Authentication, 2FA) to dodatkowe zabezpieczenie konta, które oprócz hasła wymaga drugiego elementu potwierdzającego tożsamość użytkownika.

Przykład

Aby zalogować się do konta, trzeba podać:

1. Hasło (coś, co znasz)
2. Dodatkowy kod lub potwierdzenie (coś, co masz)

Dlaczego samo hasło to za mało?

Podatność haseł

Hasła mogą zostać zgadnięte, wykradzione lub przejęte przez cyberprzestępców.

Wycieki danych

Coraz częściej zdarzają się wycieki danych logowania z dużych serwisów (np. LinkedIn, Dropbox).

Skuteczna ochrona

Cyberprzestępcy potrafią obejść proste zabezpieczenia – 2FA skutecznie ich powstrzymuje.

Jak działa 2FA?

Kod jednorazowy

Kod z SMS-a wysyłany na Twój telefon po wpisaniu hasła.

Aplikacja mobilna

Kod z aplikacji (np. Google Authenticator, Microsoft Authenticator) generowany co 30 sekund.

Powiadomienie

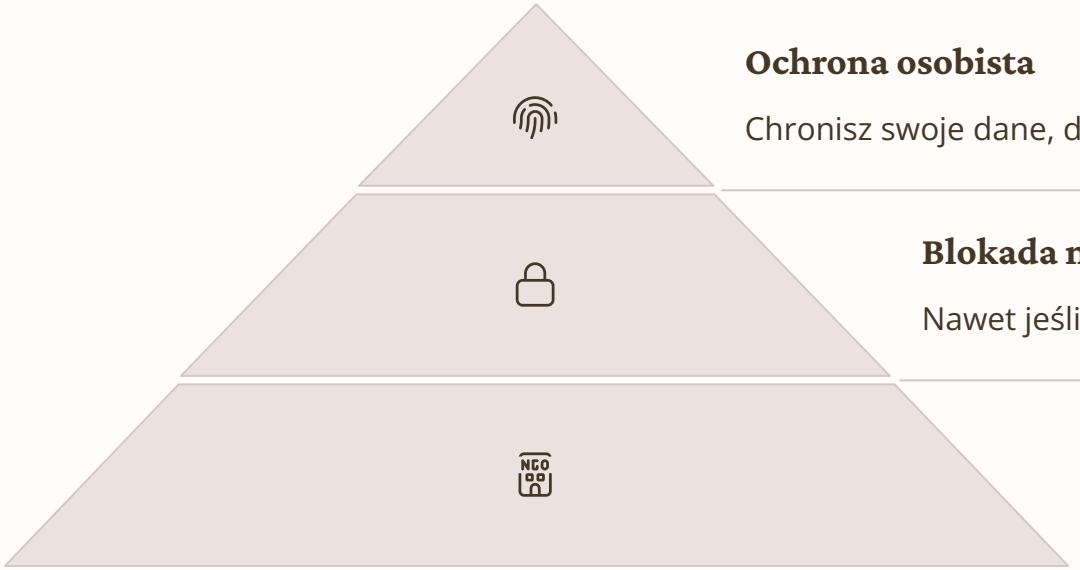
Zatwierdzenie logowania w aplikacji (np. powiadomienie na telefonie).

Sprzęt i biometria

Kod z tokena sprzętowego lub biometryczne potwierdzenie (odcisk palca, twarz).

Kod zmienia się co kilkadziesiąt sekund, więc nawet jeśli ktoś zna Twoje hasło – nie zaloguje się bez drugiego składnika.

Dlaczego warto włączyć 2FA?



Ochrona osobista

Chronisz swoje dane, dokumenty, pocztę i finanse

Blokada nieautoryzowanego dostępu

Nawet jeśli ktoś pozna Twoje hasło – nie zaloguje się

Zwiększasz bezpieczeństwo całej organizacji

Wzmacniasz ochronę konta służbowego, prywatnego i systemów firmowych. Pamiętaj, że jedno słabe ogniwo może narazić innych na niebezpieczeństwo.

Gdzie warto stosować 2FA?

Poczta e-mail

np. Gmail, Outlook

Chmura

np. Google Drive, OneDrive, Dropbox

Konta służbowe

Systemy firmowe

Komunikatory

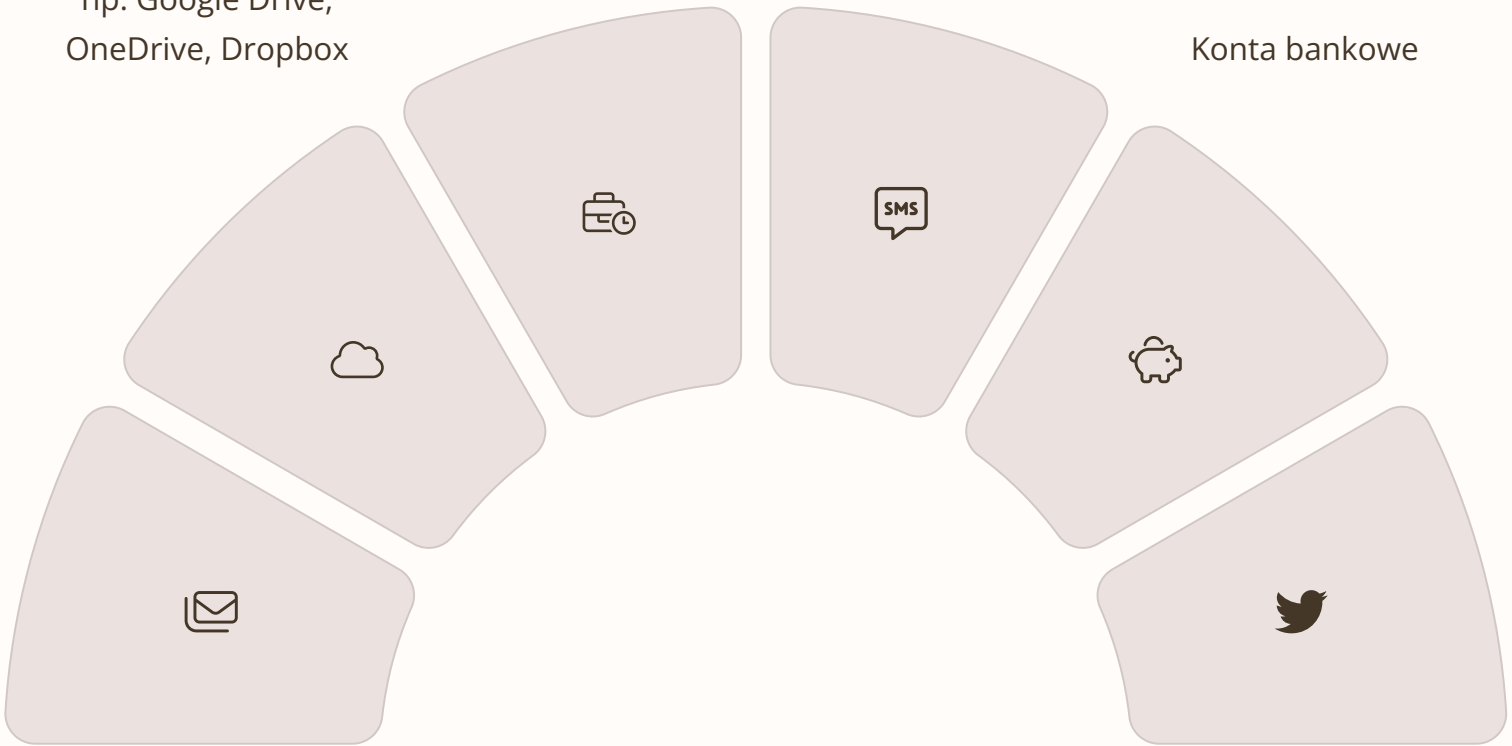
np. Teams

Bankowość

Konta bankowe

Media społecznościowe

np. Facebook, Instagram, Twitter



Wskazówki dla użytkownika

Włącz 2FA wszędzie, gdzie to możliwe

Skonfiguruj uwierzytelnianie dwuskładnikowe we wszystkich ważnych serwisach, które oferują taką możliwość.

Zapisz kody zapasowe

Przechowuj kody zapasowe w bezpiecznym miejscu – przydadzą się, gdy zgubisz telefon.

Zabezpiecz aplikację uwierzytelniającą

Chroń aplikację generującą kody dodatkowym hasłem lub biometrią.

Nie udostępniaj kodów nikomu

Nigdy nie podawaj kodów 2FA innym osobom – nawet jeśli ktoś podaje się za administratora.

Podsumowanie – dlaczego 2FA działa?

1

Ochrona przy przejęciu hasła

Chroni nawet gdy przestępca pozna Twoje hasło

2

Trudne do obejścia

Stanowi skuteczną barierę dla cyberprzestępców

3

Dostępność

Dostępne za darmo w wielu serwisach

4

Łatwość użycia

Szybkie i proste w codziennym stosowaniu

Uwierzytelnianie dwuskładnikowe to obecnie jeden z najskuteczniejszych sposobów na zabezpieczenie Twoich kont. Wdrożenie 2FA zwiększa bezpieczeństwo nie tylko Twoje, ale również całej organizacji, w której pracujesz.