Uwierzytelnianie dwuskładnikowe konta

Kompleksowy przewodnik konfiguracji kluczy U2F dla różnych platform

Uwierzytelnianie dwuskładnikowe konta w Facebook

Należy skonfigurować dwa klucze do jednego konta. Jeden klucz będzie Twoim kluczem głównym, drugi będzie kluczem zapasowym na wypadek utraty klucza głównego. Klucz zapasowy należy schować w bezpiecznym miejscu.

1. Wejdź na podany adres https://www.facebook.com/settings/?tab=your_facebook_information lub kliknij w zdjęcie swojego profilu i przejdź do "Ustawienia i prywatność".
2. Kliknij w przycisk "Ustawienia"
3. Zjedź w dół strony w poszukiwaniu panelu "Hasło i zabezpieczania".
4. Kliknij w przycisk "Uwierzytelnianie dwuskładnikowe".

1	Wybierz swój profil, do którego ma być przypisany klucz U2F. W przypadku większej liczby kont, powtórz czynności zgodnie z poniższą instrukcją. Dotyczy to tylko kont Facebook.
2	Kliknij w przycisk "Klucze zabezpieczeń".
3	Kliknij w przycisk "Dodaj".

Kliknij w przycisk "Zarejestruj klucz zabezpieczeń".

Zgodnie z instrukcją, włóż klucz U2F do portu USB.

Otrzymasz komunikat w miejscu zapisania klucza dostępu. Wybierz "Klucz zabezpieczeń".

Wprowadź kod PIN – hasło do Twojego klucza U2F.

Otrzymasz komunikat, w którym potwierdzasz konfigurację klucza U2F. Kliknij w przycisk "OK".

Dotknij złoty krążek umieszczony na kluczu.

Uwierzytelnianie dwuskładnikowe Proton Mail konta w Proton

Należy skonfigurować dwa klucze do jednego konta. Jeden klucz będzie Twoim kluczem głównym, drugi będzie kluczem zapasowym na wypadek utraty klucza głównego. Klucz zapasowy należy schować w bezpiecznym miejscu.

1

Wejdź na podany adres https://account.proton.me/ pl/mail i zaloguj się do swojego konta Proton. Kliknij w symbol ustawienia – "koło zębate", a następnie "Wszystkie ustawienia".

2

Kliknij przycisk "Konto i hasło", a następnie przejdź przez proces włączenia Uwierzytelnienia dwuskładnikowego. Należy zacząć od dodania aplikacji uwierzytelniającej. Po udanej operacji możesz skonfigurować klucz U2F.

3

Odznacz pole przy "Klucz bezpieczeństwa", a następnie potwierdź rozpoczęcie procesu poprzez podanie swojego hasła oraz 6-cyfrowego kodu z aplikacji uwierzytelniającej.

4

Przejdź przez proces konfiguracji zgodnie z kolejnymi krokami. Kliknij przycisk "Kontynuuj".

1

Otrzymasz komunikat w miejscu zapisania klucza dostępu. Wybierz "Klucz zabezpieczeń".

2

Otrzymasz komunikat, w którym potwierdzasz konfigurację klucza U2F. Kliknij w przycisk "OK".

3

Zgodnie z instrukcją, włóż klucz U2F do portu USB.

4

Wprowadź kod PIN – hasło do Twojego klucza U2F.

5

Dotknij złoty krążek umieszczony na kluczu.

6

Nadaj nazwę swojego klucza.

Otrzymasz powiadomienie o tym, że klucz został dodany pomyślnie.

Uwierzytelnianie dwuskładnikowe konta w Twitter

Należy skonfigurować dwa klucze do jednego konta. Jeden klucz będzie Twoim kluczem głównym, drugi będzie kluczem zapasowym na wypadek utraty klucza głównego. Klucz zapasowy należy schować w bezpiecznym miejscu.

Wejdź na podany adres https://twitter.com/settings/account lub do ustawień, klikając kolejno w przycisk "Więcej", a następnie "Ustawienia i prywatność".

Kliknij w przycisk "Bezpieczeństwo i dostęp do konta", a następnie w przycisk "Bezpieczeństwo".

Kliknij w przycisk "Dwustopniowa weryfikacja logowania".

Kliknij w kwadracik na wysokości wiersza "Klucz zabezpieczający", będziesz poproszony o potwierdzenie swojej tożsamości poprzez ponowne wpisanie hasła.

1. Kliknij w przycisk "Rozpocznij".
2. Kliknij w przycisk "Dodaj klucz" i postępuj zgodnie z instrukcjami.
3. Otrzymasz komunikat, w którym potwierdzasz konfigurację klucza U2F. Kliknij w przycisk "OK".
4. Zgodnie z instrukcją, włóż klucz U2F do portu USB.
5. Wprowadź kod PIN hasło do Twojego klucza U2F.
6. Dotknij złoty krążek umieszczony na kluczu.
7. Nadaj nazwę swojego klucza i kliknij w przycisk "Dalej". Instalacja klucza U2F zakończyła się pomyślnie.

Możesz uzyskać kod zapasowy, klikając przycisk "Uzyskaj kod zapasowy", który może być pomocny jako jedna z form uwierzytelniania. Druga forma wygenerowania kodu zapasowego znajduje się w panelu "Dwustopniowa weryfikacja logowania".

Uwierzytelnianie dwuskładnikowe konta w WP

Należy skonfigurować dwa klucze do jednego konta. Jeden klucz będzie Twoim kluczem głównym, drugi będzie kluczem zapasowym na wypadek utraty klucza głównego. Klucz zapasowy należy schować w bezpiecznym miejscu.

Kroki konfiguracji WP:

1

Wejdź na podany adres https://llogin.wp.pl/profil/ bezpieczeństwo i zaloguj się do swojego konta Poczty WP lub kliknij w swoją nazwę konta po prawej stronie ekranu, a następnie kliknij w przycisk "Zarządzaj kontem".

2

Po lewej stronie będziesz mieć widoczny panel. Kliknij w przycisk "Bezpieczeństwo".

3

Po prawej stronie wyszukaj panel "Logowanie dwustopniowe". Kliknij w przycisk "Zabezpiecz swoje konto".

4

Otrzymasz powiadomienie. Po zapoznaniu się z zawartą instrukcją kliknij w przycisk "Chcę zabezpieczyć moje konto".

5

Następnie potwierdź swoją tożsamość wpisując hasło do poczty. Masz do wyboru trzy sposoby logowania. Kliknij w przycisk "Logowanie kluczem bezpieczeństwa".

6

Wyświetli się panel usługi dodawania klucza U2F. Kliknij w przycisk "Dalej".

7

Nadaj nazwę swojego klucza.

8

Klucz należy mieć obok siebie, aby móc włożyć go do portu USB. Kliknij w przycisk "Dodaj klucz".

9

Otrzymasz komunikat w miejscu zapisania klucza dostępu. Wybierz "Klucz zabezpieczeń".

10

Otrzymasz komunikat, w którym potwierdzasz konfigurację klucza U2F.

11

Zgodnie z instrukcją, włóż klucz U2F do portu USB.

12

Wprowadź kod PIN - hasło do Twojego klucza U2F.

13

Dotknij złoty krążek umieszczony na kluczu.

14

Po udanej rejestracji klucza otrzymasz komunikat. Wraz z tym komunikatem otrzymasz klucze awaryjne, tj. kod, który będziesz mógł użyć, gdy nie będziesz posiadał przy sobie klucza U2F.

15

Uwierzytelnianie dwuskładnikowe konta w ONET

Należy skonfigurować dwa klucze do jednego konta. Jeden klucz będzie Twoim kluczem głównym, drugi będzie kluczem zapasowym na wypadek utraty klucza głównego. Klucz zapasowy należy schować w bezpiecznym miejscu.

Kroki konfiguracji ONET:

1

Wejdź na podany adres https://konto.onet.pl/dashboard i zaloguj się do swojego konta Poczty Onet lub kliknij w swój adres mailowy po prawej stronie ekranu i wybierz "Ustawienia konta", a następnie "Strona główna".

2

Zjedź w dół strony w poszukiwaniu panelu "Kontrola bezpieczeństwa" i kliknij w przycisk "Przejdź".

3

Zjedź w dół strony w poszukiwaniu panelu "Weryfikacja dwuetapowa" i kliknij w przycisk "Włącz".

4

Po kliknięciu masz dwie możliwości zabezpieczenia. Kliknij w przycisk "Klucz U2F".

5

Po kliknięciu w "Klucz U2F" pokazuje się okienko "Dodawania klucza USB". Kliknij w przycisk "Dalej".

6

Otrzymasz komunikat w miejscu zapisania klucza dostępu. Wybierz "Klucz zabezpieczeń".

7

Otrzymasz komunikat, w którym potwierdzasz konfigurację klucza U2F. Kliknij w przycisk "OK".

8

Zgodnie z instrukcją, włóż klucz U2F do portu USB.

9

Wprowadź kod PIN - hasło do Twojego klucza U2F.

10

Dotknij złoty krążek umieszczony na kluczu.

11

Otrzymasz powiadomienie o tym, że klucz został dodany pomyślnie.

12

Uwierzytelnianie dwuskładnikowe konta w Google

Należy skonfigurować dwa klucze do jednego konta. Jeden klucz będzie Twoim kluczem głównym, drugi będzie kluczem zapasowym na wypadek utraty klucza głównego. Klucz zapasowy należy schować w bezpiecznym miejscu.

1. Wejdź na podany adres https://myaccount.google.com i zaloguj się do swojego konta Google.
2. Przejdź do ustawień "Bezpieczeństwo" (https://myaccount.google.com/security).
3. Na dole strony poszukaj panelu "Sposób logowania się w Google". Kliknij w przycisk "Klucze dostępu". Zostaniesz poproszony o ponowne wpisanie hasła w celu potwierdzenia swojej tożsamości.
4. Kliknij w przycisk "Utwórz klucz".
5. Otrzymasz komunikat o utworzeniu klucza do konta Google. Kliknij przycisk "Użyj innego urządzenia".
6. Otrzymasz komunikat w miejscu zapisania klucza dostępu. Wybierz "Klucz zabezpieczeń".
7. Otrzymasz dwa komunikaty, przy których za każdym razem klikasz "OK", wyrażając kolejno zgodę na konfigurację i instalację klucza.
8. Zgodnie z instrukcją, włóż klucz U2F do portu USB.
9. Wprowadź kod PIN – hasło do Twojego klucza U2F.
10. Dotknij złoty krążek umieszczony na kluczu.
11. Instalacja klucza U2F zakończyła się pomyślnie.

yubico

Uwierzytelnianie dwuskładnikowe konta w Yubico

Należy skonfigurować dwa klucze do jednego konta. Jeden klucz będzie Twoim kluczem głównym, drugi będzie kluczem zapasowym na wypadek utraty klucza głównego. Klucz zapasowy należy schować w bezpiecznym miejscu.

1. Wejdź na stronę https://www.yubico.com/support/download/yubikey-manager/. Pobierz i zainstaluj YubiKey Manager odpowiedni do Twojego systemu operacyjnego.
2. PIN, który jest nadany fabrycznie to ciąg cyfr od 1 do 6 ("123456") i należy go od razu zmienić. Aby to zrobić kliknij w przycisk "Applications/PIV".
3. Kliknij w przycisk "Configure PINs" przy "PIN Managment".
4. Kliknij w przycisk "Change PIN" przy "PIN".
5. Wpisz nadany fabrycznie kod PIN ("123456"), a następnie wprowadź swój kod PIN.
6. Po wpisaniu swojego kodu PIN, otrzymasz komunikat "Changed PIN".
7. Aby ustawić kod PIN FIDO2, należy kliknąć w przycisk "Applications/FIDO2".
8. Kliknij w przycisk "Set PIN".
9. Wpisz nowy PIN FIDO2, może być to fraza lub ciąg znaków, następnie zatwierdź.
10. Po wpisaniu PIN-u otrzymasz powiadomienie, że ustawienie FIDO2 PIN zostało zakończone.

*

1. Jeśli tracisz kod PIN FIDO2 do swojego klucza, będziesz mógł go ponownie skonfigurować. Spowoduje to jednak utratę wszsytkich danych do kont, które zostały poprzednio ustawione. Proces konfiguracji musisz przejść ponownie zgodnie z instrukcją instalacji U2F. Kliknij w przycisk "Applications" i wybierz opcję "FIDO2".
2. Kliknij przycisk "Reset FIDO".
3. Pojawi się komunikat o utracie wszystkich danych zapisanych na kluczu FIDO2.
4. Kliknij przycisk "Yes". Pojawi się komunikat o konieczności wyjęcia i ponownego włożenia klucza YubiKey.
5. Dotknij złoty krążek na kluczu.
6. Pojawi się informacja, że FIDO2 zostało zresetowane. Następnie kliknij przycisk "Set PIN" i ustaw nowy PIN FIDO2.
7. Wpisz nowy PIN FIDO2, może być to fraza lub ciąg znaków, następnie zatwierdź.
8. Po wpisaniu nowego PIN-u otrzymasz powiadomienie, że ustawienie FIDO2 PIN zostało ukończone.

NIGDY NIKOMU NIE UDOSTĘPNIAJ KODU PIN DO SWOJEGO KLUCZA!