Uwierzytelnienie dwuskładnikowe (2FA) – co to jest i dlaczego warto z niego korzystać?

Bezpieczeństwo danych jest obecnie jednym z najważniejszych zagadnień w dziedzinie technologii informacyjnych. Wraz z rozwojem cyfrowego świata, wzrasta również liczba zagrożeń, z jakimi muszą zmierzyć się użytkownicy. Dlatego też coraz większą wagę przykłada się do zabezpieczania dostępu do różnych systemów i kont. Jednym z najskuteczniejszych środków ochrony jest uwierzytelnienie dwuskładnikowe.

Uwierzytelnianie dwuskładnikowe zapewnia „podwójne sprawdzanie", że naprawdę jesteśmy osobą, za którą się podajemy, gdy korzystamy z usług online. Samo hasło, to często zbyt mało, aby ochronić dostęp do naszego konta. Niezależnie od tego, czy mówimy o koncie w banku, w serwisie społecznościowym, w sklepie internetowym czy w państwowej usłudze zdrowotnej – warto aby do logowania dodać drugi składnik. W ten sposób znacznie podniesiemy poziom bezpieczeństwa tego konta.

Uwierzytelnianie dwuskładnikowe, nazywane w skrócie - 2FA, to proces bezpieczeństwa, który weryfikuje użytkowników za pomocą dwóch różnych form identyfikacji. Drugim składnikiem może być kod wysyłany SMS-em/e-mailem lub za pośrednictwem dedykowanej aplikacji mobilnej. Może to być także wcześniej wygenerowana lista kodów, którą otrzymujemy w bezpiecznym miejscu, sprzętowy klucz zabezpieczeń (U2F) czy zaawansowane dane biometryczne, np. tęczówka oka, próbka głosu, identyfikacja twarzy.

Głównym celem stosowania uwierzytelnienia dwuskładnikowego jest zwiększenie poziomu bezpieczeństwa. Hasła jednoczynnikowe, które są powszechnie używane, mogą zostać łatwo złamane w przypadku, gdy osoba trzecia zdobędzie dostęp do nich. Przykładowo, jeśli ktoś przechwyci nasze hasło podczas transmisji przez internet, może uzyskać nieuprawniony dostęp do naszego konta. Uwierzytelnienie dwuskładnikowe utrudnia takie próby, ponieważ wymaga podania dodatkowego czynnika, który nie jest dostępny dla potencjalnego atakującego.

Innym ważnym celem uwierzytelnienia dwuskładnikowego jest ochrona przed atakami typu phishing. Ataki phishingowe polegają na podszywaniu się pod zaufane instytucje lub usługi w celu wyłudzenia poufnych informacji od użytkowników. Osoba podszywająca się pod np. pracownika banku może poprosić o podanie hasła i loginu, a następnie wykorzystać te dane do włamania się na konto. W przypadku uwierzytelnienia dwuskładnikowego, atak phishingowy staje się znacznie trudniejszy, ponieważ oprócz hasła atakujący musiałby również posiadać drugi, unikalny czynnik uwierzytelniający.

Uwierzytelnienie dwuskładnikowe znalazło szerokie zastosowanie w wielu dziedzinach, gdzie istnieje potrzeba zabezpieczenia dostępu do ważnych danych lub systemów tj.: usługi bankowe, konta email, media społecznościowe, aplikacje mobilne, dostęp do danych medycznych czy usługi chmurowe.

Istnieje wiele powodów, dla których warto stosować uwierzytelnienie dwuskładnikowe. Pierwszym z nich jest ochrona przed atakami siłowymi. Ataki siłowe polegają na automatycznym testowaniu dużej liczby kombinacji haseł w celu odgadnięcia prawidłowego. Uwierzytelnienie dwuskładnikowe utrudnia tego rodzaju ataki, ponieważ nawet jeśli atakujący odkryje poprawne hasło, nie będzie w stanie uzyskać dostępu bez drugiego czynnika uwierzytelniającego.

Uwierzytelnienie dwuskładnikowe może również ułatwić zarządzanie kontami w przypadku zgubienia hasła lub konieczności resetowania dostępu. Istniejące konto może być szybko i bezpiecznie odzyskane dzięki drugiemu czynnikowi uwierzytelniającemu, np. kodowi wysłanemu na zarejestrowany numer telefonu.

W niektórych branżach istnieją regulacje i standardy, które wymagają wprowadzenia dodatkowych środków bezpieczeństwa, takich jak uwierzytelnienie dwuskładnikowe. Przykładem może być sektor finansowy, zdrowotny lub rządowy, które muszą spełniać określone wymagania dotyczące ochrony danych.

Spośród wielu dostępnych sposobów na wzmocnienie swojego bezpieczeństwa w sieci, uwierzytelnianie dwuskładnikowe możemy zaliczyć do jednego z ważniejszych. Stosując takie zabezpieczenie, mocno utrudnimy działania cyberprzestępców, którzy chcieliby włamać się na nasze konto.

Pamiętajmy jednak, że bezpieczeństwo naszych danych zależy głównie od nas samych!

***

Program sektorowy „Bankowcy dla Edukacji" to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Zapraszamy na stronę **www.bde.wib.org.pl**

BANKOWCY
DLA EDUKACJI
program sektorowy