Bezpieczeństwo Twoich kont

Jeśli chodzi o logowanie do ważnych kont internetowych, bezpieczeństwo powinno być zawsze priorytetem. Do ważnych kont niewątpliwie należy skrzynka pocztowa i wszystkie konta, na których masz pieniądze. Bez wątpienia dotyczy to również kont na portalu GLOCIN. Jeśli to możliwe, koniecznie włącz weryfikację dwuetapową przy każdym logowaniu.

W praktyce logowanie odbywa się w taki sposób, że oprócz hasła musisz wprowadzić dodatkowy kod, który jest generowany automatycznie przez Google Authenticator. Następnie wprowadzasz ten kod podczas logowania. Następnie w portalu Glocin wprowadzasz ten kod podczas potwierdzania transakcji i zmian. Nowy kod jest generowany co 30 sekund. Nie musisz się jednak martwić, że nie zdążysz go użyć. Każdy wygenerowany kod jest ważny przez 30 sekund po jego wygaśnięciu.

Sam proces logowania zajmuje kilka sekund dłużej, ale Twoje konto jest o wiele bezpieczniejsze i nawet jeśli teoretycznie ktoś pozna Twoje hasło, nie wystarczy ono aby się zalogować.

Jak działa Google Authenticator

Aplikacja Google Authenticator automatycznie generuje sześciocyfrowe kody potrzebne do zalogowania się na różne konta.
Kody te zmieniają się regularnie i są trwale połączone bezpośrednio z Twoim telefonem.

Aby dostać się do Twojego konta, ktoś potrzebowałby zarówno znajomości hasła, jak i fizycznego dostępu do Twojego telefonu. Podnosi to poziom bezpieczeństwa, a każda próba przejęcia kontroli nad Twoim kontem jest bardziej skomplikowana dla potencjalnych napastników.

Weryfikacja dwuetapowa za pomocą aplikacji Google Authenticator

Gdzie pobrać aplikację Google Authenticator?

Aplikacja Google Authenticator jest dostępna na urządzenia mobilne z systemami Android oraz iOS, można ją pobrać zarówno w Google Play, jak i App Store:

Pobierz aplikację Google Authenticator z Google Play

Pobierz aplikację Google Authenticator z App Store

Jak włączyć weryfikację dwuetapową (2FA)

Włączenie weryfikacji dwuetapowej jest bardzo proste. Postępuj według instrukcji:

1. Po zalogowaniu się do portalu Glocin przejdź do swojego profilu, a w zakładce zabezpieczenia wybierz opcję włączenia weryfikacji dwuetapowej. Ta opcja jest

zwykle proponowana już podczas rejestracji, znajdziesz ją także w zakładce „Security”/„Bezpieczeństwo”.

2. Wyświetli się kod QR, który służy do skojarzenia Twojego konta z telefonem.

3. Pobierz i włącz aplikację Google Authenticator na telefonie i kliknij na czerwone kółko z symbolem + znajdujące się w prawym dolnym rogu.

4. Wybierz opcję skanowania kodu kreskowego – zostanie uruchomiony aparat, który należy naprowadzić na kod QR.

5. Kod QR zostanie wczytany przez aplikację Google Authenticator, a konto zostanie powiązane bezpośrednio z Twoim telefonem.

6. Podczas logowania do portalu Glocin lub innej usługi, należy włączyć aplikację Google Authenticator i wprowadzić wygenerowany kod.

Co się stanie, jeśli zgubię telefon lub usunę aplikację Google Authenticator?

Aplikacja Google Authenticator nie jest bezpośrednio powiązana z Twoim kontem Google i nie jest synchronizowana z żadnym urządzeniem. To zapewnia Ci bezpieczeństwo, ponieważ do uzyskania kodu musisz mieć przy sobie telefon komórkowy, z którego możesz przepisać kod. Z drugiej strony, jeśli telefon zostanie zgubiony lub aplikacja zostanie usunięta, nie jest możliwe odzyskanie połączonych kont poprzez ponowną instalację.

Po włączeniu weryfikacji dwuetapowej za pomocą aplikacji Google Authenticator zostanie wygenerowany prywatny kod, który można wprowadzić bezpośrednio do Google Authenticator. Wróć do instrukcji, w punkcie 4 zamiast kodu QR możesz wybrać opcję Wprowadzenie dostarczonego klucza.

Zachowaj wygenerowany prywatny kod 2fa w bezpiecznym miejscu, najlepiej zapisz go na kartce i ukryj. Jeśli usuniesz aplikację i nie masz dostępu do tego kodu, uzyskanie dostępu do portalu Glocin lub innej usługi jest zazwyczaj bardzo skomplikowane, konieczne będzie udowodnienie, że naprawdę jesteś właścicielem konta.

Co zrobić, jeśli kupię nowy telefon komórkowy lub muszę przenieść aplikację Google Authenticator na inny telefon?

W obu przypadkach, jeśli masz telefon z aktywną aplikacją Google Authenticator, możesz postępować w następujący sposób.

- Pierwszym i najłatwiejszym sposobem jest zalogowanie się do portalu Glocin, przejście do swojego profilu, w karcie/zakładce bezpieczeństwo w dolnej części znajduje się opcja pokazująca aktualny klucz. Wpisz kod z aplikacji Google Authenticator, skojarzony z tym kontem w portalu i kliknij na wyświetl klucz prywatny. Portal pokaże Ci Twój klucz prywatny i kod QR, dzięki czemu możesz przenieść swój login na inny lub dodatkowy telefon.

- Drugi, bardziej skomplikowany sposób, polega na ręcznym wprowadzeniu kodu prywatnego, który wcześniej starannie przepisałeś i bezpiecznie przechowałeś, do nowego urządzenia.

Bezpieczne przechowywanie nie oznacza zapisywania w e-mailach, zdjęciach, na pulpicie, w portfelu, w dzienniku itp. Myśl o bezpieczeństwie, w przeciwnym razie stracisz swoje pieniądze.