Wstęp

W Avivie Twoje bezpieczeństwo traktujemy niezwykle poważnie. Gdy korzystasz z naszych serwisów internetowych zależy ono w dużej mierze także od Ciebie. Jak odpowiednio przygotować się i na co zwracać uwagę, aby pozostać bezpiecznym korzystając z naszych serwisów?

Odpowiedzi znajdziesz w niniejszym poradniku. Prosimy o zapoznanie się z podstawowymi zasadami bezpieczeństwa, które pomogą Ci uchronić się od ataku cyberprzestępców i utraty poufnych danych. Pamiętaj, że aby pozostać bezpiecznym w sieci, należy zachowywać się uważnie i podobnie jak na drodze – stosować zasadę ograniczonego zaufania.

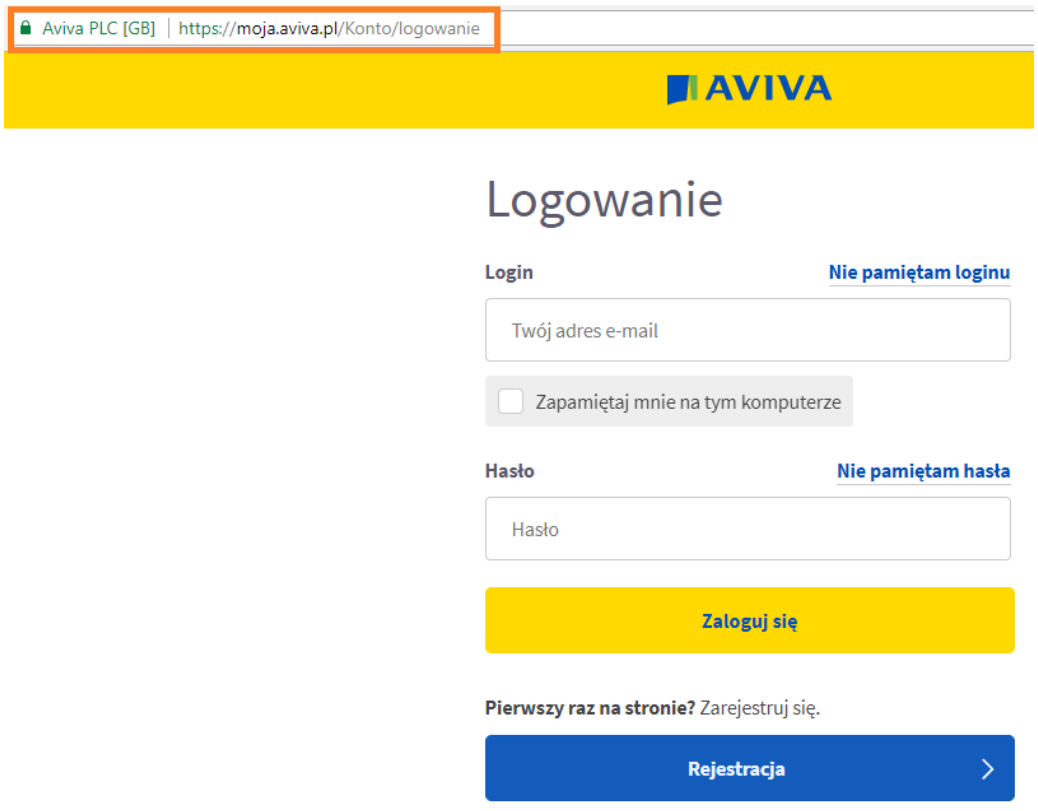
Bezpieczne logowanie i przechowywanie hasła

Logowanie

Do serwisów internetowych Aviva loguj się zawsze przez stronę **www.aviva.pl** lub poprzez wpisanie bezpośredniego adresu aplikacji (**https://moja.aviva.pl/Konto/logowanie**) w oknie przeglądarki.

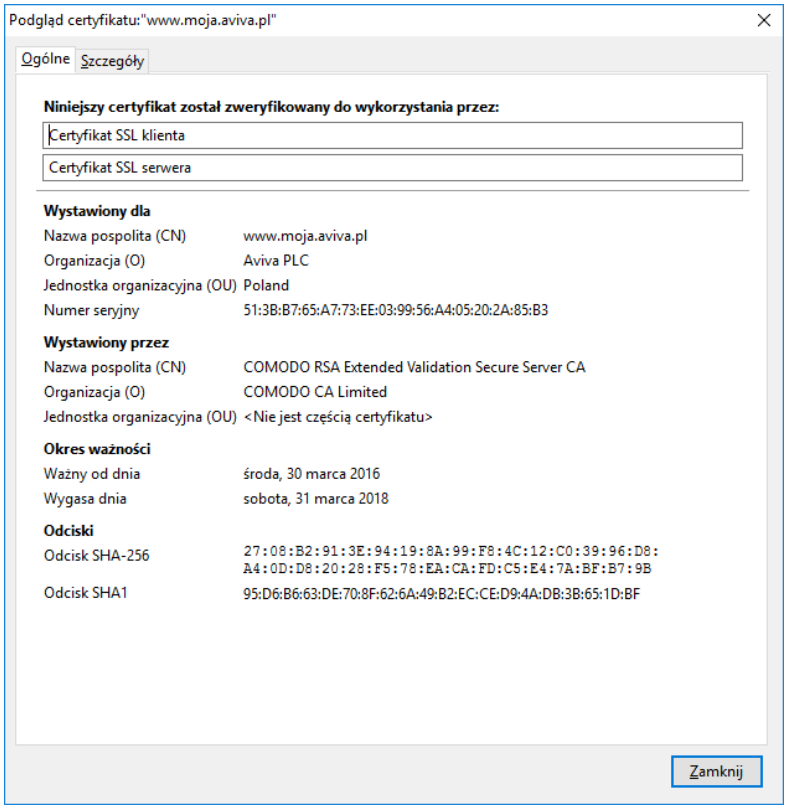
Nigdy nie loguj się korzystając z linków przesłanych na Twój adres e-mail oraz przez linki z wyszukiwarki internetowej. Przestępcy często podszywają się pod różnego rodzaju instytucje i próbują wykorzystać zaufanie oraz nieuwagę klientów.

Zawsze sprawdzaj, czy adres strony logowania zaczyna się od liter **https (a nie http)** oraz czy jest poprzedzony symbolem zamkniętej kłódki. Jeżeli go nie ma – nie loguj się i ponownie dokładnie sprawdź wprowadzony adres. Przestępcy mogą skutecznie preparować strony w celu wyłudzenia danych do logowania.



Certyfikat bezpieczeństwa

Sprawdź również, czy strona jest zabezpieczona ważnym certyfikatem wystawionym dla **moja.aviva.pl**, w tym celu kliknij na symbol zamkniętej kłódki poprzedzający adres strony. Informacje o certyfikacie powinny wyglądać następująco:



Pamiętaj, że nasze serwisy nigdy nie proszą o instalację dodatkowych certyfikatów, ani jakiegokolwiek innego oprogramowania na Twoim urządzeniu. Jest to szczególnie ważne, gdyż instalując niepożądany certyfikat lub aplikację, możesz otworzyć potencjalny dostęp do urządzenia narażając bezpieczeństwo swoich danych.

Do korzystania z naszych serwisów potrzebujesz wyłącznie urządzenia z dostępem do Internetu oraz przeglądarki internetowej.

Po zakończeniu korzystania z aplikacji należy wylogować się poprzez kliknięcie przycisku „wyloguj”. Odradzamy zamykanie aplikacji poprzez samo zamknięcie okna przeglądarki.

Jak stworzyć dobre hasło?

Stosuj hasła trudne do odgadnięcia, będące kombinacją co najmniej 8 znaków, zawierające:
- duże i małe litery
- cyfry
- znaki specjalne

Unikaj stosowania haseł składających się np. z Twojej daty urodzenia, nazwy użytkownika, numeru telefonu lub innych osobistych informacji.

Po wpisaniu loginu i hasła na stronie logowania unikaj korzystania z oferowanej przez przeglądarki funkcji „zapamiętywania haseł”. Staraj się również nie zapisywać ich w formie papierowej. Hasła zapisane w plikach powinny być zawsze zaszyfrowane. Jeżeli na swoim urządzeniu posiadasz plik z danymi do logowania, korzystanie z sieci P2P skutecznie obniża poziom ich bezpieczeństwa.

Nigdy nie udostępniaj swoich danych logowania osobom trzecim, nie przechowuj ich w ogólnodostępnych miejscach i dbaj o to, by były regularnie zmieniane. Zmień hasło zawsze gdy masz podejrzenie, że ktoś uzyskał do niego dostęp.

Pamiętaj również, że Aviva nigdy nie prosi o przesłanie Twojej nazwy użytkownika oraz hasła. Zwróć szczególną ostrożność gdy dostaniesz taką prośbę oraz poinformuj nas o tym fakcie pod numerem infolinii: 22 563 28 02

Bezpieczeństwo urządzeń

W celu zminimalizowania zagrożeń związanych z bezpieczeństwem w Internecie upewnij się, że właściwie zabezpieczyłeś i przygotowałeś do tego swoje urządzenie.

- Korzystaj jedynie ze sprawdzonych i zaufanych urządzeń, unikaj logowania z publicznie dostępnych sprzętów oraz sieci; w tym niezabezpieczonych sieci publicznych np. w kawiarniach czy centrach handlowych
- Używaj legalnie zakupionego oprogramowania oraz aktualizuj je do najnowszych wersji producenta. Dotyczy to zarówno systemu operacyjnego jak również przeglądarek internetowych
- Stosuj oprogramowanie ochronne przeciwko wirusom, malware, upewnij się że korzystasz z ochrony firewall
- Instaluj jedynie aplikacje pochodzące z wiarygodnych źródeł: AppStore (dla systemu iOS), Google Play (dla systemu Android), Windows Phone Store lub Windows Store (dla systemów Windows). W przypadku instalacji aplikacji na urządzenia mobilne sprawdź od jakiego wydawcy pochodzi
- Chroń swój sprzęt przed niepowołanym dostępem fizycznym. Zabezpiecz swój profil w systemie operacyjnym stosując hasło oraz blokadę ekranu w przypadku urządzeń mobilnych
- Uważnie sprawdzaj komunikaty wyświetlane w systemie i serwisach internetowych
- Nie otwieraj podejrzanych wiadomości i linków wysyłanych przez nieznanych nadawców. To najpopularniejsza metoda infekcji urządzeń wirusami

Jeżeli nie jesteś pewien czy Twoje urządzenie jest prawidłowo zabezpieczone zalecamy kontakt ze specjalistami lub profesjonalnymi firmami informatycznymi.

Popularyzacja Internetu oraz dostępu do internetowych serwisów transakcyjnych niesie za sobą wiele udogodnień jak również zagrożeń. Z roku na rok rośnie również liczba cyberprzestępców, przypadków wyłudzeń lub kradzieży poufnych danych oraz środków.

Wierzymy, że powyższe wskazówki pozwolą zminimalizować ryzyka związane z korzystaniem z internetowych serwisów oraz pozwolą Wam na bezpieczne korzystanie z sieci.

Pamiętaj, że Twoje bezpieczeństwo w sieci zależy głównie od Ciebie!