



Drogi Kliencie,

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.

1. Bezpieczne logowanie i przechowywanie hasła

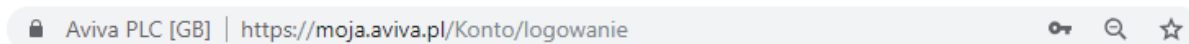
1.1 Logowanie

Do serwisów internetowych Aviva loguj się zawsze przez stronę <https://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, gdy nie zweryfikowałeś nadawcy 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. Poniżej poprawny wygląd zamkniętej kłódki dla poszczególnych przeglądarek:

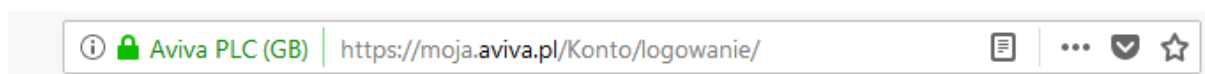
Chrome



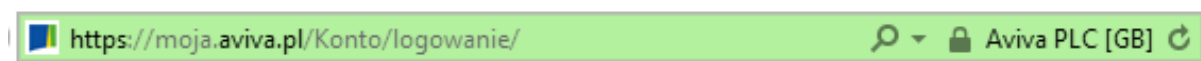
Chrome – urządzenie mobilne z systemem Android



Firefox



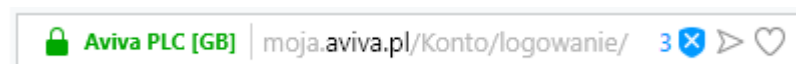
Internet Explorer



Microsoft Edge



Opera



Safari



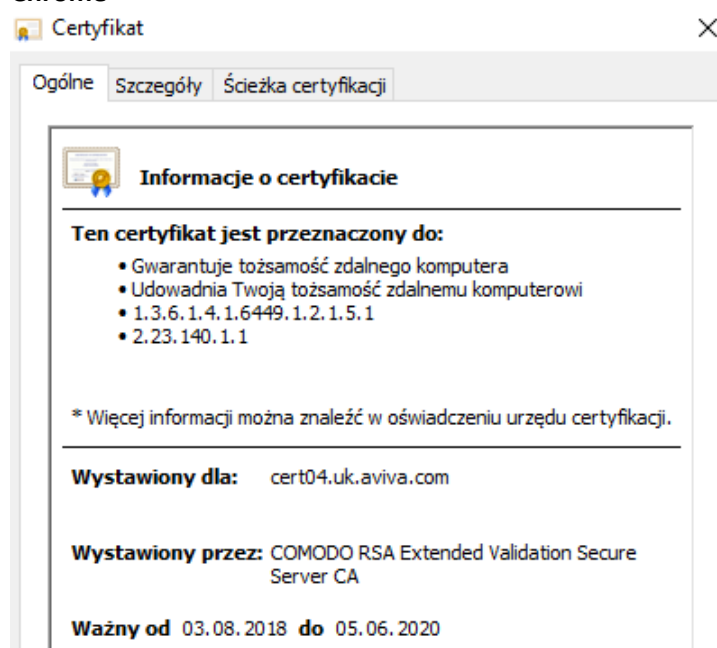
Safari – urządzenie mobilne z systemem iOS



1.2 Certyfikat bezpieczeństwa

Sprawdź również, czy strona jest zabezpieczona ważnym certyfikatem wystawionym dla serwisu **Moja Aviva**, w tym celu kliknij na symbol zamkniętej kłódki poprzedzający adres strony. Informacje o certyfikacie powinny wyglądać jak poniżej. Przykłady dla najpopularniejszych przeglądarek:

Chrome



Firefox

Podgląd certyfikatu: „cert04.uk.aviva.com”

Ogólne Szczegóły

Niniejszy certyfikat został zweryfikowany do wykorzystania przez:

- Certyfikat SSL klienta
- Certyfikat SSL serwera

Wystawiony dla

Nazwa pospolita (CN)	cert04.uk.aviva.com
Organizacja (O)	Aviva PLC
Jednostka organizacyjna (OU)	Digital
Numer seryjny	00:85:6C:AF:ED:CA:A5:57:AF:89:64:8B:4D:A5:D7:AD:37

Wystawiony przez

Nazwa pospolita (CN)	COMODO RSA Extended Validation Secure Server CA
Organizacja (O)	COMODO CA Limited
Jednostka organizacyjna (OU)	<Nie jest częścią certyfikatu>

Okres ważności

Ważny od dnia	piątek, 3 sierpnia 2018
Wygasa dnia	piątek, 5 czerwca 2020


Odciski

Odcisk SHA-256	7F:5F:58:11:E0:E3:72:66:78:72:55:33:01:D7:6F:90:F5:B2:33:B8:6C:05:23:4D:4D:1C:45:A7:21:72:2C:16
Odcisk SHA1	84:85:08:AB:47:6E:F4:2B:67:A6:8F:FB:D6:E8:7E:AC:90:CF:F4:C3

Internet Explorer

Certyfikat

Ogólne Szczegóły Ścieżka certyfikacji

 **Informacje o certyfikacie**

Ten certyfikat jest przeznaczony do:

- Gwarantuje tożsamość zdalnego komputera


* Więcej informacji można znaleźć w oświadczeniu urzędu certyfikacji.

Wystawiony dla: cert04.uk.aviva.com

Wystawiony przez: COMODO RSA Extended Validation Secure Server CA

Ważny od 03.08.2018 **do** 05.06.2020

Opera



Informacje o certyfikacie

Ten certyfikat jest przeznaczony do:

- Gwarantuje tożsamość zdalnego komputera
- Udowadnia Twoją tożsamość zdalnemu komputerowi
- 1.3.6.1.4.1.6449.1.2.1.5.1
- 2.23.140.1.1

* Więcej informacji można znaleźć w oświadczeniu urzędu certyfikacji.

Wystawiony dla: cert04.uk.aviva.com

Wystawiony przez: COMODO RSA Extended Validation Secure Server CA


Ważny od 03.08.2018 **do** 05.06.2020

Safari

COMODO RSA Certification Authority

COMODO RSA Extended Validation Secure Server CA

cert04.uk.aviva.com



cert04.uk.aviva.com
Issued by: COMODO RSA Extended Validation Secure Server CA
Expires: Friday, 5 June 2020 at 01:59:59 Central European Summer Time
✔ This certificate is valid

▶ Trust
▶ Details

Hide Certificate

OK

Pamiętaj, że nasze serwisy nigdy nie proszą o instalację dodatkowych certyfikatów, ani żadnego 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 i przeglądarki internetowej.

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

1.3 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: 22 557 44 44

2. 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 nieznaną 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.