
Zasady bezpieczeństwa

Logowanie do systemów AXA

1. Przed wprowadzeniem na stronie logowania swojego użytkownika i hasła upewnij się że:
 - a. W pasku adresu przeglądarki znajduje się adres:
<https://www.axaonline.pl/ofe/login.xhtml>.
 - b. W pasku adresu przeglądarki widoczny jest symbol kłódki wskazujący na to że połączenie jest szyfrowane.
 - c. Certyfikat został wystawiony dla witryny *.axa-polska.pl, jest zaufany i nie upłynął jego termin ważności.
 - d. Jakikolwiek ostrzeżenie dotyczące certyfikatów mogą oznaczać próbę oszustwa i wyłudzenia informacji, należy w takim przypadku zrezygnować z logowania i skontaktować się z CENTRUM KLIENTA (<https://axa.pl/centrum-klienta/>).

Autoryzacja transakcji:

1. Niektóre transakcje (np. zmiana hasła, numeru telefonu) mogą wymagać potwierdzenia jednorazowym hasłem sms. Nie jest to hasło które używamy do logowania.
2. AXA nigdy nie prosi o podanie jednorazowego hasła sms, w sytuacjach innych niż potwierdzenie ww. transakcji.

Bezpieczeństwo haseł:

1. Twoje hasło jest tajne. Nie należy nikomu przekazywać tych haseł, także pracownikom czy agentom AXA.
2. Pracownicy AXA nigdy nie proszą o podanie hasła do logowania lub jednorazowego hasła sms.
3. Aplikacje AXA nigdy proszą o podanie lub potwierdzenie hasła lub danych osobowych. Aplikacje żądają hasła wyłącznie w procesie logowania (hasło nr 1), potwierdzania transakcji (jednorazowe hasło sms), lub zmiany hasła. Jeśli aplikacja prosi o podanie/potwierdzenie hasła lub danych osobowych może to oznaczać próbę oszustwa i wyłudzenia informacji, należy w takim przypadku powstrzymać się od wprowadzenia danych i skontaktować się z CENTRUM KLIENTA (<https://axa.pl/centrum-klienta/>).
4. Jeśli Twoje hasło zostało zmienione na Twoją prośbę przez AXA – zmień je natychmiast.
5. Nie zapisuj swoich haseł – pamiętaj je!
6. Nie zezwalaj przeglądarce na zapamiętywanie Twoich haseł (odpowiedz „nie” na monit z przeglądarki).
7. Twórz hasła trudne do zgadnięcia a łatwe do zapamiętania. Dobre hasło powinno:
 - a. Zawierać powyżej 8 znaków.
 - b. Zawierać małe i wielkie litery, cyfry lub znaki specjalne.
 - c. Zalecamy korzystanie z tzw. „*passphrase*” czyli haseł składających się z łatwej do zapamiętania frazy lub krótkiego zdania – hasło takie jest praktycznie niemożliwe do złamania a łatwe do zapamiętania.
8. Zmieniaj okresowo swoje hasło.
9. Zachowaj ostrożność przy korzystaniu z oprogramowania i serwisów internetowych służących do przechowywania haseł (elektronicznych portfeli), Twoje hasła są najbezpieczniejsze w Twojej głowie.
10. Zalecane jest cykliczne czyszczenie danych w przeglądarce.

Wiadomość E-mail od AXA

1. AXA nigdy nie prosi swoich Klientów (e-mailem, listownie lub telefonicznie) o podanie danych pozwalających na zalogowanie do serwisu AXA On-Line, w szczególności loginu i hasła. dostępu. W celu weryfikacji tożsamości Klienta możemy prosić o podanie danych osobowych (PESEL, imię i nazwisko) oraz danych dot. umowy ubezpieczenia (numer polisy, numer rachunku).

2. AXA nigdy nie prosi o odwiedzenie jakiegokolwiek strony ani nie przesyła w poczcie e-mail odnośników do stron (linków).
 3. AXA nigdy nie informuje pocztą e-mail o zmianie numerów konta AXA i innych informacji związanych z płatnościami.
 4. W przypadku informacji od AXA o braku wymaganej płatności, należy dokonywać wpłat na numer konta podany na polisie.
 5. Jeśli otrzymali Państwo podejrzaną wiadomość sugerującą powiązanie z AXA prosimy o zgłoszenie tego faktu do CENTRUM KLIENTA (<https://axa.pl/centrum-klienta/>).
-