



więcej / niż standard

Zasady bezpieczeństwa dla użytkowników serwisów internetowych AXA

Informacje podstawowe

Korzystanie z usług elektronicznych dostępnych w Internecie może wiązać się z ryzykiem związanym z bezpieczeństwem Twoich danych. AXA dokłada wszelkich starań, żeby zapewnić należyty poziom bezpieczeństwa, ale zależy ono także od Ciebie. Dlatego pamiętaj o kilku zasadach, które zmniejszą zagrożenie podczas korzystania z usług elektronicznych:

- Zwracaj uwagę na komunikaty, adresy i certyfikaty wyświetlane na stronach WWW.
- Upewnij się, że logowanie do serwisów WWW następuje poprzez zaszyfrowany kanał.
- Uważaj na próby wyłudzenia danych (tzw. *phishing*) - zwracaj uwagę na przesyłane do Ciebie linki (odnośniki) a przed ich użyciem upewnij się, że pochodzą z zaufanego źródła.
- Loguj się do serwisów WWW z urządzeń, które znasz i o których wiesz, że są bezpieczne.
- Chroń dostęp do własnych urządzeń.
- Instaluj na swoim urządzeniu aplikacje pochodzące wyłącznie z zaufanych źródeł.
- Aktualizuj system operacyjny i oprogramowanie antywirusowe na swoim urządzeniu.
- Twórz unikalne i silne hasła, którymi będziesz uwierzytelniać się przy logowaniu. Nie udostępniaj hasel nikomu.
- Łącz się z Internetem i loguj do serwisów WWW tylko przez wiarygodne i zabezpieczone sieci WI-FI.

Wszelkie incydenty dotyczące bezpieczeństwa elektronicznych kanałów dostępu AXA (np. ataki oparte o technikę „*phishing*”) możesz zgłosić bezpośrednio na adres: bezpieczenstwo@axa.pl. Pamiętaj, żeby podać jak najwięcej szczegółów sprawy, w tym zwłaszcza której spółki AXA / którego kanału dostępu dotyczy zdarzenie.

Bardziej szczegółowe wskazówki dotyczące bezpieczeństwa znajdziesz poniżej.

Logowanie do systemów AXA

Przed wprowadzeniem na stronie logowania nazwy użytkownika (loginu) i hasła upewnij się, że:

- W pasku adresu przeglądarki adres zaczyna się od <https://>
- W pasku adresu przeglądarki jest widoczny symbol kłódki wskazujący na to, że połączenie jest szyfrowane.
- Certyfikat został wystawiony dla witryny w jednej z domen: *.axa.pl, *.axadirect.pl, *.axa-polska.pl, *.axaubezpieczenia.pl, *.axatravel.pl – oraz, że jest zaufany i nie upłynął termin jego ważności. Pamiętaj, że aplikacje AXA mogą być także niekiedy umieszczone w domenach uprawnionych Partnerów AXA. W razie wątpliwości – skontaktuj się z nami.

Wiadomości e-mail lub SMS od AXA

Pamiętaj kilka rzeczy dotyczących wiadomości e-mail lub SMS:

- AXA nigdy nie prosi swoich klientów (e-mailem, listownie lub telefonicznie) o podanie danych pozwalających zalogować się do aplikacji AXA, w szczególności loginu i hasła dostępu;
- AXA nigdy nie informuje pocztą e-mail o zmianie numerów kont AXA i innych informacji związanych z płatnościami.
- Jeśli otrzymasz wiadomość z plikiem lub linkiem (odnośnikiem), upewnij się, że została ona wysłana przez zaufanego nadawcę i była przez Ciebie oczekiwana. Jeśli nie jesteś w stanie tego zweryfikować – nie klikaj w odnośniki i nie otwieraj plików.

Bezpieczeństwo haseł

- Twoje hasło jest poufne. Nie należy nikomu go przekazywać, także pracownikom czy agentom AXA.
- Pracownicy AXA nigdy nie proszą o podanie hasła do logowania.
- Aplikacje AXA żądają hasła wyłącznie w procesie logowania.
- Jeśli jesteś dodatkowo proszony 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 z AXA.
- Jeśli Twoje hasło zostało zmienione na Twoją prośbę przez AXA – zmień je potem natychmiast na własne.
- Nie zezwalaj przeglądarce na zapamiętywanie Twoich haseł (odpowiedz „nie” na monit przeglądarki).
- Zmieniaj okresowo swoje hasło.
- Twórz hasła trudne do zgadnięcia ale łatwe do zapamiętania. Dobre hasło powinno:
 - zawierać co najmniej 8 znaków;
 - zawierać małe i wielkie litery, cyfry i znaki specjalne.

Im dłuższe i trudniejsze hasło, tym trudniej je odgadnąć lub złamać z użyciem dedykowanego oprogramowania.

Bezpieczeństwo urządzenia

Korzystaj z urządzeń (komputer, smartphone, tablet) w sposób bezpieczny. W tym celu:

- Unikaj korzystania z serwisów WWW AXA na komputerach lub sieciach współdzielonych z innymi osobami - np. w kafejkach internetowych, hotelach.
- Uważaj na połączenia poprzez publicznie dostępne sieci WiFi – korzystaj tylko z rozpoznanych i zaufanych punktów dostępowych; w razie wątpliwości łącz się z serwisem WWW przy użyciu dodatkowego oprogramowania szyfrującego (VPN).
- Po zakończeniu korzystania z konta internetowego AXA - wyloguj się z niego.
- Zabezpiecz komputer hasłem lub innym mechanizmem uwierzytelniającym.
- Stosuj system antywirusowy z aktualnymi sygnaturami wirusów.
- W przypadku poczty elektronicznej - korzystaj z dodatkowego systemu antyspamowego.
- Aktualizuj system operacyjny, przeglądarkę i inne oprogramowanie na urządzeniu.
- Korzystaj z firewall'a (zapory ogniowej) na urządzeniu.
- Pobieraj pliki i programy wyłącznie z zaufanych źródeł.

- Zachowaj ostrożność przy korzystaniu z nośników z nieznanymi źródłami (płyty, pendrive itp.) – mogą one zawierać szkodliwe oprogramowanie.
- Unikaj korzystania z oprogramowania do wymiany plików (P2P) - pobierane pliki mogą być szkodliwym oprogramowaniem.
- Nigdy nie zapisuj haseł na dysku komputera, w notatkach, e-mailach itp.

Jak rozpoznać próbę oszustwa?

Częstym działaniem przeciw użytkownikom są obecnie oszustwa (tzw. *scam*) polegające na próbie wyłudzenia danych lub haseł, bądź próbie sprowokowania do instalacji szkodliwego oprogramowania (tzw. „*phishing*”). Do wyłudzeń używany jest najczęściej SPAM w postaci wiadomości e-mail lub SMS, ale może być to także rozmowa, w której przestępca stosuje techniki psychologiczne. Stosowanie się do poniższych zaleceń pozwoli zminimalizować ryzyko ataku:

- Uważaj na wiadomości informujące o okazjach otrzymania atrakcyjnego wynagrodzenia za pracę czy zakup produktów po niespodziewanie korzystnej cenie.
- Instytucje finansowe nie proszą w wiadomościach e-mail lub SMS o podanie danych osobowych lub haseł swoich klientów.
- Jeśli otrzymałeś w wiadomości informację zawierającą numer konta do wpłaty, zawsze zweryfikuj tę informację i źródło jej pochodzenia przed dokonaniem wpłaty. Pamiętaj – instytucje finansowe nie praktykują przesyłania takich informacji e-mailem.
- Zachowaj czujność rozmawiając przez telefon z osobą, która podając się za przedstawiciela/pracownika AXA pyta o Twoje dane osobowe. Jeśli nie jesteś pewien tożsamości dzwoniącego, skontaktuj się AXA.
- Ostrożnie podchodź do prośby nieznanymi osobami o instalację czegośkolwiek na Twoim komputerze lub kliknięcie w odnośnik – może być to próba zawirusowania Twojego komputera.
- Nie podawaj swoich haseł, pinów i danych osobowych, gdy rozmawiasz przez telefon w miejscu publicznym (np. w pociągu) – ktoś może je podsłuchać i wykorzystać.
- Ostrożnie korzystaj z sieci społecznościowych (np. Facebook, Twitter). Nie publikuj zbyt wielu danych o sobie w Internecie. Takie dane można wykorzystać do przygotowania skutecznej próby wyłudzenia.