Zasady bezpieczeństwa

Baza wiedzy

Bezpieczeństwo w Internecie w dużej mierze zależy od Ciebie. Pamiętaj o kilku zasadach, które zmniejszą zagrożenia podczas korzystania z usług elektronicznych.

1. Loguj się rozważnie
   Zwracaj uwagę na komunikaty, adresy witryn, certyfikaty.
2. Zachowaj czujność
   Cokolwiek wzbudzi Twoje podejrzenia, skontaktuj się z Centrum Telefonicznej Obsługi Klienta.
3. Nie otwieraj stron logowania z linku w wiadomości e-mail.
4. Loguj się z urządzeń, które są bezpieczne.
   Unikaj logowania z cudzego sprzętu.
5. Instaluj aplikacje tylko z zaufanych źródeł.
6. Aktualizuj oprogramowanie oraz bazy wirusów.
7. Twórz unikalne hasło i nie zdradzaj go nikomu.
8. Nie udostępniaj swoich prywatnych danych nieznajomym.
9. Nie używaj publicznej sieci WI-FI do logowania.

Logowanie do systemów AXA

Przed wprowadzeniem na stronie logowania swojego użytkownika 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 *.axa-polska.pl, jest zaufany i nie upłynął termin jego ważności;
- jakiekolwiek ostrzeżenia dot. certyfikatów mogą oznaczać próbę oszustwa i wyłudzenia informacji, należy w takim przypadku zrezygnować z logowania i skontaktować się z Centrum Telefonicznej Obsługi Klienta.

Wiadomość e-maila od AXA

Pamiętaj kilka rzeczy dotyczących wiadomości e-mail:

- 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 prosi o odwiedzenie jakiejkolwiek strony ani nie przesyła w poczcie e-mail odnośników do stron (linków);
- AXA nigdy nie informuje pocztą e-mail o zmianie numerów konta AXA i innych informacji związanych z płatnościami;
- jeśli otrzymasz podejrzaną wiadomość sugerującą powiązanie z AXA, prosimy o zgłoszenie tego faktu do Centrum Telefonicznej Obsługi Klienta.

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.
3. Aplikacje AXA nigdy nie proszą o podanie lub potwierdzenie hasła lub danych osobowych. Aplikacje AXA żądają hasła wyłącznie w procesie logowania.
4. 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
5. i skontaktować się z Centrum Telefonicznej Obsługi Klienta.
6. Jeśli Twoje hasło zostało zmienione na Twoją prośbę przez AXA – zmień je natychmiast.
7. Nie zapisuj swoich haseł – pamiętaj je.
8. Nie zezwalaj przeglądarce na zapamiętywanie Twoich haseł (odpowiedz „nie" na monit przeglądarki).
9. Zmieniaj okresowo swoje hasło.
10. Zachowaj ostrożność przy korzystaniu z oprogramowania i serwisów internetowych służących do przechowywania haseł (elektronicznych portfeli). Twoje hasła są najbezpieczniejsze w Twojej głowie.
11. Twórz hasła trudne do zgadnięcia, a łatwe do zapamiętania. Dobre hasło powinno:
    - zawierać co najmniej 9 znaków,
    - zawierać małe i wielkie litery, cyfry lub znaki specjalne (3 z 4 kategorii).
12. 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.

Bezpieczeństwo komputera

Jak zadbać o komputer? Komputer, z którego korzystasz powinien być należycie zabezpieczony. Należy unikać korzystania z konta internetowego AXA na komputerach współdzielonych z innymi osobami (np. w kafejkach internetowych, hotelach, hotspotach). Po zakończeniu korzystania z konta internetowego AXA wyloguj się oraz wyczyść pliki tymczasowe w przeglądarce.

W celu zabezpieczenia swojego komputera należy:

- zabezpieczyć komputer hasłem,
- stosować system antywirusowy i antyspyware z aktualnymi sygnaturami wirusów,
- korzystać z systemu antyspamowego,
- aktualizować system operacyjny, przeglądarkę i inne oprogramowanie,
- korzystać z firewall'a na własnym komputerze,
- pobierać pliki i programy wyłącznie z zaufanych źródeł,
- zachować ostrożność przy korzystaniu z nośników z nieznanych źródeł (płyty, pendrive itp.) – mogą one zawierać wirusy,
- zachować ostrożność przy otwieraniu poczty od nieznanych nadawców – załączniki lub treść mogą zawierać wirusy,
- unikać korzystania z oprogramowania do wymiany plików (P2P), pobierane pliki mogą być zawirusowane,
- nigdy nie zapisywać haseł na dysku komputera, w notatkach, e-mailach itp.

Jak rozpoznać próbę oszustwa?

Wyłudzenie danych lub haseł jest bardzo częstym atakiem na użytkowników korzystających z aplikacji internetowych. Stosowanie się do poniższych zaleceń pozwoli zminimalizować ryzyko padnięcia ofiarą takiego ataku.

- Uważaj na wiadomości informujące o okazjach atrakcyjnego wynagrodzenia za pracę czy zakup produktów po niespodziewanie korzystnej cenie. Mogą być one próbą wyłudzenia Twoich danych lub oszustwem.
- Instytucje finansowe nie proszą w wiadomościach e-mail o podanie danych osobowych lub haseł swoich klientów. Taka wiadomość może być próbą oszustwa.
- 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 przesyłanie takich informacji e-mailem.
- Wiadomości e-mail od instytucji finansowych zazwyczaj są podpisywane cyfrowo.
- 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 z Centrum Telefonicznej Obsługi Klienta. Pamiętaj również, że profesjonalna firma dzwoniąc do swojego klienta uprzedza go nagrywaniu rozmowy, co ma podnieść bezpieczeństwo obsługi klienta.
- Ostrożnie podchodź do prośby od nieznanych osób o instalacje czegokolwiek na Twoim komputerze lub kliknięcie w odnośnik – zazwyczaj jest to próba zawirusowania Twojego komputera. Nie podawaj swoich tele-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 łatwo wykorzystać przeciwko Tobie.