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://eagent.axa-polska.pl/.
    b. W pasku adresu przeglądarki widoczny jest symbol kłódki wskazujący na to że połączenie jest szyfrowane. Jak to zrobić?
    c. Certyfikat został wystawiony dla witryny *.axa-polska.pl, jest zaufany i nie upłynął jego termin ważności. Jak to zrobić?
    d. Jakiekolwiek ostrzeżenia dotyczące certyfikatów mogą oznaczać próbę oszustwa i wyłudzenia informacji, należy w takim przypadku zrezygnować z logowania i skontaktować się z 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 proszą o podanie lub potwierdzenie hasła lub danych osobowych. Aplikacja eAgent żąda 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 i skontaktować się z CENTRUM TELEFONICZNEJ OBSŁUGI KLIENTA.
5. Jeśli Twoje hasło zostało zmienione na Twoją prośbę przez AXA – zmień je natychmiast.
6. Nie zapisuj swoich haseł – pamiętaj je!
7. Nie zezwalaj przeglądarce na zapamiętywanie Twoich haseł (odpowiedz „nie” na monit z przeglądarki).
8. Twórz hasła trudne do zgadnięcia a łatwe do zapamiętania. Dobre hasło powinno:
    a. Zawierać co najmniej 9 znaków.
    b. Zawierać małe i wielkie litery, cyfry lub znaki specjalne (3 z 4 kategorii).
    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
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.

Wiadomość E-mail od AXA

1. AXA nigdy nie prosi swoich Klientów (e-mailem, listownie lub telefonicznie) o podanie danych pozwalających na zalogowanie do aplikacji AXA, w szczególności loginu i hasła dostępu.
2. AXA nigdy nie prosi o odwiedzenie jakiejkolwiek 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. Jeśli otrzymali Państwo podejrzaną wiadomość sugerującą powiązanie z AXA prosimy o zgłoszenie tego faktu do CENTRUM TELEFONICZNEJ OBSŁUGI KLIENTA**.**

Bezpieczeństwo komputera:

1. 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).
2. Po zakończeniu korzystania z konta internetowego AXA wyloguj się oraz wyczyść pliki tymczasowe w przeglądarce. Jak to zrobić?

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

Jak rozpoznać próbę oszustwa?

Wyłudzenia 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.

1. 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.
2. Instytucje finansowe nie proszą w wiadomościach e-mail o podanie danych osobowych lub haseł swoich klientów. Taka wiadomość może być próbą oszustwa.
3. Jeśli otrzymałeś w wiadomości informację zawierającą numer konta do wpłaty – zawsze weryfikuj tę informację i źródło jej pochodzenia przed dokonaniem wpłaty. Pamiętaj – instytucje finansowe nie praktykują przesyłania takich informacji e-mailem.
4. Wiadomości e-mail od instytucji finansowych zazwyczaj są podpisane cyfrowo.
5. 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 o nagrywaniu rozmowy, co ma podnieść bezpieczeństwo obsługi klienta.
6. Ostrożnie podchodź do prośby od nieznanych osób o instalację czegokolwiek na twoim komputerze lub kliknięcie na odnośnik – zazwyczaj jest to próba zawirusowania Twojego komputera.
7. Nie podawaj swoich tele-pinów i danych osobowych, gdy rozmawiasz przez telefon w miejscu publicznym (np. w pociągu) – ktoś może je podsłuchać i wykorzystać.
8. Ostrożnie korzystaj z sieci społecznościowych (np. Facebook, Twitter). Nie publikuj zbyt wielu danych o sobie w Internecie. Takie dane można łatwo wykorzystać przeciwko Tobie.