Informacje o zasadach bezpiecznego korzystania z Serwisu Transakcyjnego ING TFI24

Dokładamy wszelkich starań, aby zapewnić poprawne działanie niniejszego serwisu transakcyjnego. Naszym priorytetem jest zagwarantowanie bezpieczeństwa Twoich danych, dlatego stale pracujemy nad rozwiązaniami zwiększającymi bezpieczeństwo korzystania z niniejszego serwisu transakcyjnego, wdrażając rozwiązania zgodne z najnowszymi standardami bezpieczeństwa. Bezpieczeństwo jednak zależy nie tylko od poziomu zabezpieczeń stosowanych przez nas, ale przede wszystkim od Ciebie i Twoich działań w Internecie, dlatego ważne jest abyś zapoznał się z poniższymi zasadami bezpiecznego korzystania z serwisów internetowych. Jeśli masz wątpliwości dotyczące bezpieczeństwa serwisu transakcyjnego ING TFI24 lub zauważyłeś, że aplikacja działa nieprawidłowo, natychmiast skontaktuj się z Infolinią Funduszy Inwestycyjnych ING.

W jaki sposób my dbamy o Twoje bezpieczeństwo

W celu zapewnienia maksymalnego bezpieczeństwa podczas korzystania z serwisu transakcyjnego wprowadziliśmy następujące rozwiązania:

- **Szyfrowane połączenie internetowe** przy użyciu technologii Transport Layer Security (TLS), zapewniającej poufność oraz integralność transmisji danych. Serwer prezentuje certyfikat z kluczem 2048 bitowym podpisany algorytmem SHA-256, co zapewnia najwyższy poziom bezpieczeństwa łączności. Technologia ta pozwala na dostęp do rejestrów funduszy inwestycyjnych bez konieczności zakupu dodatkowego oprogramowania zabezpieczającego. Wymagane jest używanie przeglądarki, która obsługuje protokół TLS 1.2 wraz z szyfrowaniem algorytmem AES z kluczem minimum 256-bit.
- **Automatyczne kończenie nieaktywnych sesji** polegające na automatycznym wylogowaniu z systemu transakcyjnego użytkownika w razie bezczynności w systemie przez zdefiniowany okres czasu.
- **Szyfrowanie wrażliwych danych** przechowywanych w bazach.

W jaki sposób Ty możesz zwiększyć swoje bezpieczeństwo

Poniżej przedstawiamy podstawowe zasady bezpiecznego korzystania z serwisów internetowych od stosowania, których zależy bezpieczeństwo Twoich danych i zgromadzonych środków.

Bezpieczeństwo komputera

- Korzystaj z serwisu transakcyjnego tylko na zaufanych urządzeniach (komputer, tablet, telefon etc.) z zainstalowanym legalnym systemem operacyjnym.
- Pamiętaj aby regularnie aktualizować posiadany system operacyjny oraz inne aplikacje (w szczególności przeglądarki internetowe, klientów poczty, przeglądarki pdf itp.). Aktualizacje legalnego oprogramowania często naprawiają luki w bezpieczeństwie, które starają się wykorzystać oszuści.
- Używaj zapory ogniowej (firewall), która pomaga chronić komputer przed atakami z sieci.
- Używaj programu antywirusowego z najnowszymi definicjami wirusów.
- Chroń swój system pocztowy przed przychodzącym spamem.

- Należy zachowywać dużą ostrożność podczas pobierania jakichkolwiek plików z Internetu czy otwierania załączników do wiadomości e-mail, bez względu na to, od kogo one pochodzą.
- Przestrzegamy przed używaniem oprogramowania pochodzącego z nielegalnego czy niezaufanego źródła. Nie należy instalować nieznanych programów otrzymanych pocztą elektroniczną lub pobranych z niezaufanych witryn www.
- Należy cyklicznie skanować urządzenia programami antywirusowymi.
- Należy unikać korzystania z aplikacji transakcyjnej ingtfi24 za pośrednictwem niesprawdzonych połączeń (np. kafejki internetowe, publiczne WiFi).
- Należy korzystać z najnowszych wersji przeglądarek internetowych. Zalecane wersje:
  - Microsoft Edge – wersja poprzednia i najnowsza
  - Mozilla Firefox – wersja poprzednia i najnowsza
  - Google Chrome – wersja poprzednia i najnowsza
  - Opera – wersja poprzednia i najnowsza.

Bezpieczeństwo serwisu transakcyjnego

- Zawsze ręcznie wpisuj adres URL serwisu transakcyjnego: https://ingtfi24.pl
- Sprawdź, czy na pewno korzystasz z bezpiecznego protokołu https.
- Sprawdź, czy połączenie jest szyfrowane - świadczy o tym ciąg „https://" i wyświetlany symbol zamkniętej kłódki (w pasku adresu lub na dole strony).
- Kliknij w symbol kłódki i przekonaj się, czy certyfikat bezpieczeństwa jest aktualny.
- Upewnij się, że na stronie nie występują podejrzane elementy.
- Nie uruchamiaj Systemu korzystając z załączników lub linków otrzymanych pocztą e-mail oraz z linków znajdujących się na stronach internetowych o podejrzanym adresie.
- Nie odpowiadaj na e-maile dotyczące prośby o weryfikację Twoich danych, a w szczególności nie przesyłaj pocztą elektroniczną swoich danych identyfikacyjnych (np. identyfikator, hasło) ani żadnych innych ważnych informacji.
- Po zalogowaniu sprawdź, czy data ostatniego logowania odpowiada dacie, kiedy korzystałeś z usługi.
- Nie korzystaj z funkcji „kopiuj-wklej" przy wprowadzeniu numerów rachunków bankowych.

Bezpieczne hasło

- Bezpieczne hasło powinno składać się z minimum 12 znaków.
- Hasło powinno być kombinacją przynajmniej trzech liter (minimum 1 duża oraz 1 mała litera), przynajmniej dwóch cyfr oraz znaków specjalnych i nie może zawierać 3 lub więcej identycznych, następujących po sobie znaków.
- Hasło musi być różne od ostatnich 6 wprowadzonych haseł.
- Unikaj haseł odwołujących się do Twoich danych osobowych.
- Bezpieczne hasło nie może być powtarzalną kombinacją znaków.
- Hasło powinno być zmieniane cyklicznie, nie rzadziej niż raz na miesiąc.
- Unikaj używania tych samych haseł w różnych systemach.
- Nie udostępniaj swoich haseł innym osobom.
- Nie podawaj identyfikatora i hasła na żądanie innych systemów i podmiotów trzecich.
- Nie zapisuj haseł w systemach i aplikacjach w postaci możliwej do odczytania.
- Zmieniaj hasło zawsze, gdy zachodzi podejrzenie, że zostało ono ujawnione.