Zasady bezpieczeństwa korzystania z Serwisu Internetowego

1. Serwis dostępny jest pod adresem: https://moventum.com.pl/int2trigon/tfi/trigon/Login.app. Link do Serwisu Internetowego znajduje się na stronie internetowej Towarzystwa www.trigontfi.pl w zakładce „informacje i ogłoszenia".
2. Do logowania nie należy używać odnośników otrzymanych pocztą elektroniczną lub umieszczonych na innych stronach niż wskazane w ust. 1 powyżej.
3. Serwis zapewnia szyfrowane połączenie internetowe przy użyciu technologii Transport Layer Security (TLS), zapewniającej poufność oraz integralność transmisji danych. Serwer prezentuje certyfikat podpisany algorytmem SHA-256, co zapewnia najwyższy poziom bezpieczeństwa łączności.
4. Każdorazowo, przed zalogowaniem do Serwisu Internetowego należy sprawdzić czy połącznie jest bezpieczne, w szczególności czy Użytkownik korzysta z bezpiecznego protokołu „https://" oraz czy strona wyświetla odpowiedni certyfikat strony logowania. Dane o certyfikacie dostępne są w przeglądarce w pasku adresu lub na dole strony w postaci zamkniętej kłódki. Po kliknięciu na kłódkę należy kliknąć „wyświetl certyfikat" i zweryfikować prawidłowość certyfikatu SSL, sprawdzając jego dane. Dane te powinny przedstawiać wartości jak poniżej:
   1) Wystawiony dla:
      a) Nazwa pospolita (CN): www.moventum.com.pl
      b) Organizacja (O): Atlantic Fund Serivces
      c) Jednostka organizacyjna (OU): Atlantic Fund Serivces
      d) Numer seryjny: 43:D1:4F:9C:4E:89:46:9E:4C:73:78:0D:C2:99:4B:D4
   2) Wystawiony przez:
      a) Nazwa pospolita (CN): Symantec Class 3 Secure Server CA - G4
      b) Organizacja (O): Symantec Corporation
      c) Jednostka Organizacyjna (OU): Symantec Trust Network
   3) Odciski:
      a) SHA-256: 10:90:EE:88:C5:C8:47:FE:2A:27:80:A5:23:0A:8D:88:58:E2:47:0E:13:29:16:93:76:AB:25:C9:B7:FB:E8:BA
      b) SHA1: C9:7C:66:B6:DC:DB:11:2B:61:AD:CD:77:E6:90:B6:0C:AF:16:53:49
5. W przypadku trzykrotnego błędnego podania Hasła, dostęp do Serwisu Internetowego zostaje zablokowany.
6. Odblokowanie usługi internetowej możliwe jest za pośrednictwem Serwisu Internetowego. W celu odblokowania usługi, Użytkownik wybiera opcję „Odblokuj Hasło". Następnie wprowadza dane Użytkownika uprawnionego do korzystania z Serwisu. Po zatwierdzeniu danych, jeżeli wprowadzone dane są poprawne Użytkownik otrzyma nowe Hasło na zdefiniowany wcześniej adres poczty elektronicznej.
7. W celu zapewnienia bezpieczeństwa informacji zmiana Hasła przez Użytkownika jest wymuszana co 90 dni.
8. Hasło musi składać się z minimum 8 znaków, w tym min. 2 cyfr i min. 3 liter (wielkich i małych) i min. jednego znaku specjalnego. Nie należy podawać Identyfikatora i Hasła na żądanie innych systemów i podmiotów trzecich. Hasło należy zmienić zawsze, gdy zachodzi podejrzenie, że zostało ono ujawnione osobom trzecim.
9. Użytkownik powinien korzystać z Serwisu tylko na zaufanych urządzeniach (komputer, tablet, telefon etc.) z zainstalowanym legalnym systemem operacyjnym.
10. Nie należy odpowiadać na e-maile dotyczące prośby o weryfikację danych osobowych, a w szczególności nie należy przesyłać pocztą elektroniczną swoich danych identyfikacyjnych (np. identyfikator, hasło) ani żadnych innych ważnych informacji.

11. Nie należy używać oprogramowania pochodzącego z nielegalnego czy niezaufanego źródła. Nie należy instalować nieznanych programów otrzymanych pocztą elektroniczną lub pobranych z niezaufanych witryn www.
12. Zaleca się używanie zapory ogniowej (firewall), która pomaga chronić komputer przed atakami z sieci. Firewall jest jednym ze sposobów zabezpieczania komputerów, sieci i serwerów przed intruzami. Firewall może być zarówno sprzętem komputerowym ze specjalnym oprogramowaniem, bądź samym oprogramowaniem chroniącym nasz komputer przed niepowołanym dostępem z sieci. Zapora na domowym komputerze sprawdza cały ruch sieciowy wchodzący i wychodzący, ogranicza i zabrania dostępu w obydwie strony nieznanym programom lub użytkownikom.
13. Należy używać programu antywirusowego z najnowszymi definicjami wirusów.
    Wirus komputerowy jest fragmentem kodu posiadającym zdolność powielania się (tak jak prawdziwy wirus), przenoszącym się poprzez umieszczenie własnych kopii w plikach wykonywalnych. Wirus nie może działać sam - potrzebuje nosiciela w postaci innego programu komputerowego (np. ściągniętego za darmo ze strony www), po uruchomieniu którego zazwyczaj pierwszy uruchamia się złośliwy kod wirusa, a następnie właściwy program.
    Po skutecznym zainfekowaniu dalsze działanie wirusa zależy od jego typu i może obejmować:
    1) wyłudzenie danych umożliwiających realizację płatności w bankowości internetowej;
    2) kradzież tożsamości;
    3) infekcję plików podczas ich uruchamiania lub tworzenia;
    4) kasowanie lub uszkadzanie danych w systemach i plikach;
    5) kradzież danych uwierzytelniających do portali społecznościowych i kont pocztowych

    Koń trojański (popularnie nazywany trojanem) mieści się w ogólnie przyjętej definicji wirusa, ponieważ próbuje przedostać się do komputera bez wiedzy i zgody użytkownika. Koń trojański nie powiela i nie rozprzestrzenia się jednak samodzielnie, a komputer-ofiara infekowana jest tylko poprzez umyślne zainstalowanie przez użytkownika programu-nosiciela. Konie trojańskie wykonują zwykle jedną z następujących operacji:
    1) wykradanie poufnych danych i haseł.
    2) szpiegowanie działalności (np. przesyłanie do hakera wciskanych klawiszy w celu poznania hasła do poczty lub konta bankowego).
    3) utrudnianie pracy programom antywirusowym w celu osłabienia komputera.
    4) instalowanie w systemie backdoora i udostępnianie kontroli nad systemem nieuprawnionym osobom w celu rozsyłania spamu, dokonywania ataków DDoS itp.
    5) modyfikowanie naszej przeglądarki internetowej poprzez zmianę strony startowej lub instalowanie irytujących wtyczek.
    6) kasowanie danych lub uszkadzanie systemu

Wymagania techniczne

14. Wymagane jest używanie przeglądarki, która obsługuje protokół TLS 1.0 lub wyższy wraz z szyfrowaniem algorytmem AES z kluczem minimum 128-bit, lub algorytmem 3DES.
15. Należy korzystać z najnowszych wersji przeglądarek internetowych. Zalecane wersje przeglądarek:
    1) Internet Explorer – od wersji 9
    2) Mozilla Firefox – wersja poprzednia i najnowsza
    3) Google Chrome – wersja poprzednia i najnowsza
    4) Opera – od wersji 15