Ważne informacje dotyczące bezpieczeństwa

1. Bezpieczeństwo Serwisu internetowego Insignis TFI S.A.

W celu zalogowania się do Serwisu internetowego Insignis TFI S.A. należy skorzystać ze strony https://transferagent.vistra.com/Insignis/ lub poprzez przekierowanie ze strony https://www.insignistfi.pl (w górnym menu należy wybrać opcję „Dla Klientów", a następnie „Serwis internetowy").

Każdorazowo, przed zalogowaniem do Serwisu internetowego należy sprawdzić certyfikat strony logowania, aby mieć pewność, że połączenie zostało nawiązane z właściwą stroną. Dane o certyfikacie dostępne są w przeglądarce w pasku adresu strony w postaci zamkniętej kłódki. Po kliknięciu na kłódkę należy zweryfikować prawidłowość certyfikatu, sprawdzając jego następujące właściwości:

a) "Ogólne" – należy sprawdzić dla kogo i przez kogo został wystawiony certyfikat oraz datę ważności certyfikatu. Powinno być:

- Wystawiony dla: transfergent.vistra.com
- Wystawiony przez: GlobalSign RSA OV SSL CA 2018
- Okres ważności certyfikatu - ważny od 11.10.2019 do 11.10.2020

b) "Szczegóły" - tzw. Odcisk palca/Odcisk SHA1, pole to powinno mieć wartość:

f72808887074f4ab5ee6a6f02785f47dfcdb7417

c) "Ścieżka certyfikacji" lub „Hierarchia certyfikacji" (w zależności od przeglądarki internetowej) – należy sprawdzić czy ścieżka jest następująca:

GlobalSign Root CA – R3
└► GlobalSign RSA OV SSL CA 2018
└► transferagent.vistra.com

Połączenie z Serwisem internetowym Insignis TFI S.A. jest szyfrowane przy użyciu protokołu internetowego SSL z 256-bitowym kluczem szyfrującym. To gwarantuje pełne bezpieczeństwo wymiany danych między Uczestnikiem a Serwisem internetowym, pod warunkiem że Uczestnik rzeczywiście połączył się z Serwisem internetowym Insignis TFI S.A. Dodatkowo stosowanymi zabezpieczeniami są:

a) blokowanie hasła po trzech nieudanych próbach logowania,

b) automatyczne wylogowanie po piętnastominutowej bezczynności ze strony Uczestnika.

2. Wymagania techniczne.

Zalecane jest używanie przeglądarki internetowej, która umożliwia szyfrowanie z siłą 256 bitów, takiej jak np. Google Chrome lub Mozilla Firefox w najnowszej dostępnej wersji. Do prawidłowego działania aplikacji wymagane jest włączenie obsługi Javascript oraz zezwolenie na zapisywanie plików cookie w ustawieniach przeglądarki internetowej.

3. **Podstawowe zagrożenia związane z korzystaniem z usług w sieci Internet, w tym w ramach elektronicznych kanałów dostępu, to:**

1) **Phishing** - podszywanie się w celu wyłudzenia informacji, np. danych umożliwiających dostęp do serwisu internetowego (identyfikatora, hasła). Zazwyczaj są to fałszywe powiadomienia imitujące komunikaty z instytucji finansowej rozsyłane za pośrednictwem poczty elektronicznej, w których kieruje się użytkowników do zalogowania na strony internetowe naśladujące oryginalne strony instytucji finansowych, w celu przechwycenia danych do logowania.

2) **Złośliwe oprogramowanie** (ang. malware) – wszelkie aplikacje i programy wykorzystywane w celu działań przestępczych lub mające na celu wyrządzenie szkody użytkownikowi komputera, smartfonu, tableta. Do złośliwego oprogramowania należą m.in.:

a) **wirusy** – program złośliwy, który przenosi się poprzez zapis zainfekowanego pliku na nośniku danych w celu kradzieży lub usunięcia danych, zakłócenia pracy urządzenia lub przejęcia kontroli nad urządzeniem. Najczęściej do zarażenia wirusem elektronicznym dochodzi po pobieraniu plików z niezaufanego źródła lub otwarciu załącznika w poczcie elektronicznej;

b) **robaki** – złośliwe oprogramowanie podobne do wirusów, samoreplikujące się tylko poprzez sieć, niepotrzebujące programu nosiciela. Oprócz replikacji robaki mogą niszczyć plik, wysyłać pocztę lub pełnić rolę trojana;

c) **trojany** – nie rozmnażają się jak wirusy, ale ukrywają się pod nazwą lub w części pliku wykonując operacje w tle, szkodliwe dla użytkownika, np. umożliwiające przejęcie kontroli nad systemem przez nieuprawnione osoby;

d) **programy szpiegujące** (ang. spyware) – programy zbierające i przesyłające dane o użytkowniku (np. informacje o odwiedzanych witrynach, hasła dostępowe) do przestępcy. Programy szpiegujące mogą gromadzić i przekazywać dane umieszczone w urządzeniu jaki i śledzić działania użytkownika np. tekst wpisywany z klawiatury.

3) **Niechciana poczta**, tzw. **spam** – niezamawiane lub niepotrzebne wiadomości elektroniczne rozsyłane masowo do nieznanych sobie osób. Spam często wiąże się z różnego rodzaju wirusami i złośliwymi programami, powoduje zatykanie się łączy, blokuje miejsce na dyskach, spowalnia działanie serwerów.

4. **Środki ostrożności zalecane dla użytkowników Serwisu internetowego**

1) Zabezpieczenie danych wykorzystywanych do logowania

Dane dostępowe do Serwisu internetowego (identyfikator i hasło) powinny być znane tylko Uczestnikowi. Nie należy ich ujawniać osobom trzecim lub przechowywać na urządzeniu w formie, która umożliwia nieautoryzowany dostęp i odczyt. Hasło należy okresowo zmieniać.

2) Logowanie do Serwisu internetowego

Logując się do Serwisu internetowego Insignis TFI S.A. należy zawsze sprawdzać poprawność i ważność certyfikatu strony do logowania. Nie wolno ignorować ostrzeżeń generowanych przez przeglądarkę dotyczących błędnego lub nieważnego certyfikatu.
Do logowania nie należy używać odnośników otrzymanych w poczcie elektronicznej lub umieszczonych na innych stronach niż Insignis TFI S.A. Może to być próba przechwycenia danych umożliwiających zalogowanie w Serwisie internetowym (phishing).
Po zakończeniu pracy należy pamiętać o wylogowaniu się z Serwisu internetowego korzystając z funkcji *Wyloguj*.

3) Zabezpieczenie urządzeń zapewniających dostęp do Internetu

Urządzenie zapewniające dostęp do sieci Internetu (komputer stacjonarny, laptop, tablet, smartphone) powinno być zabezpieczone przez aktualny program antywirusowy, włączoną zaporę sieciową (ang. firewall), program antyszpiegowski. Należy ponadto regularnie sprawdzać, czy system operacyjny i programy zainstalowane w urządzeniu, w szczególności przeglądarki internetowe, posiadają najnowsze aktualizacje, ponieważ w atakach wykorzystywane są błędy wykryte w zainstalowanym oprogramowaniu. Zaleca się uruchomienie w przeglądarce internetowej filtrów antyphishingowych, które sprawdzają, czy wyświetlona strona internetowa jest autentyczna i nie służy wyłudzaniu informacji.
Podczas używania prywatnej sieci bezprzewodowej Wi-Fi należy ustalić bezpieczne i trudne do złamania hasło dostępu do sieci. Rekomenduje się także korzystanie z najwyższych możliwych standardów szyfrowania sieci bezprzewodowych Wi-Fi, które są możliwe do uruchomienia na posiadanym sprzęcie np. protokół WPA2.

4) Kontakt z Insignis TFI S.A.

Insignis TFI S.A. nie wysyła wiadomości elektronicznych z prośbą o podanie hasła do Serwisu internetowego lub innych poufnych danych. W przypadku otrzymania takiej wiadomości, nie należy na nią odpowiadać nadawcy oraz należy powiadomić Insignis TFI S.A. wysyłając informację na adres: biuro@insignistfi.pl.