Bezpieczeństwo logowania

Szanowni Państwo,

Informacje szczegółowe dotyczące danych naszych Klientów dostępne są jedynie po zalogowaniu – należy znać adres strony oraz podać **login i hasło** do konta **(dane niezbędne do zalogowania)**. Dane niezbędne do zalogowania należy właściwie chronić, by tylko osoby uprawnione mogły z nich korzystać.

Prosimy zwracać szczególną uwagę na odpowiednie zabezpieczenie tych danych, w szczególności:

- Należy okresowo zmieniać hasło do konta. Zalecamy stosowanie haseł zawierających wielkie/małe litery, znaki specjalne, cyfry o długości co najmniej 8 znaków.
- Nie należy przesyłać hasła za pośrednictwem poczty elektronicznej, ponieważ może zostać przechwycone przez przestępców i wykorzystane wbrew naszej woli.
- Nie należy przechowywać danych niezbędnych do zalogowania w tym samym miejscu oraz nie należy udostępniać ich innym osobom.
- Należy unikać logowania z komputerów, do których dostęp mają również inne osoby (np. w kawiarenkach, u znajomych) jak również z tabletów i telefonów należących do innych osób.
- Należy unikać logowania przy użyciu nieznanych jak również niezabezpieczonych i ogólnie dostępnych połączeń bezprzewodowych wi-fi, w ten sposób inne osoby mogą uzyskać dostęp do naszego urządzenia.
- Nie należy wchodzić na stronę logowania do systemu korzystając z odnośników otrzymanych pocztą e-mail lub znajdujących się na stronach nie należących do Towarzystwa.
- Należy korzystać wyłącznie z przycisku logowania dostępnego na stronie aplikacji. Zalecamy każdorazowe sprawdzenie, czy połączenie jest szyfrowane, o czym będzie świadczyło pojawienie się symbolu kłódki przed adresem (dodatkowo należy kliknąć na symbol kłódki w celu sprawdzenia czy nie pojawia się komunikat o błędnym certyfikacje klucza publicznego).
- Nie należy odpowiadać na żadne e-maile dotyczące weryfikacji Twoich danych (np. identyfikatora, hasła) lub innych ważnych informacji – Towarzystwo nigdy nie zwraca się o podanie danych poufnych za pomocą poczty elektronicznej.
- Należy uważnie czytać komunikaty i powiadomienia pojawiające się w trakcie logowania i korzystania z serwisu. Przestępcy potrafią podrabiać strony w internecie. Jeśli cokolwiek na stronie internetowej wzbudza podejrzenia lub wystąpiło jakiekolwiek nietypowe działanie, należy bezzwłocznie skontaktować się z Towarzystwem.

Zwracamy również uwagę na stan urządzenia, za pośrednictwem którego jesteśmy podłączeniu do aplikacji, w szczególności:

- Nie należy instalować na żądanie dodatkowego oprogramowania na komputer, tablet lub telefon – pamiętaj, że Towarzystwo nigdy o to nie prosi (szczególnie za pośrednictwem e-maili, SMS-ów lub komunikatów w serwisie internetowym). Program lub aplikacja mogą być furtką do przejęcia kontroli nad Twoim urządzeniem przez przestępców.
- Nigdy nie należy otwierać podejrzanych maili i załączników, to samo dotyczy umieszczonych w wiadomościach linków. Mogą one zainfekować każde urządzenie (komputer, tablet, telefon) wirusem.
- Urządzenie musi mieć aktualne i legalne oprogramowanie: system operacyjny, program antywirusowy oraz rekomendowaną przeglądarkę. Przestępcy mogą wykorzystać luki w oprogramowaniu. Aktualizacje legalnego oprogramowania bardzo często powoduje usunięcie błędów i dziur w oprogramowaniu co w znacznym stopniu utrudnia działania przestępców.
- Nie należy udostępniać swoich urządzeń (komputer, tablet, telefon) osobom postronnym, mogę one bez wiedzy użytkownika skopiować dane lub zainstalować/ściągnąć szkodliwe oprogramowanie, w tym wirusy.