Bezpieczeństwo logowania

1. Informacje szczegółowe dotyczące danych osobowych oraz polis dostępne są jedynie po zalogowaniu do serwisu. Dostęp do tych danych możliwy jest jedynie dla kogoś kto zna adres strony, adres e-mail i hasło do konta Użytkownika (dane niezbędne do zalogowania).
2. Hasło do konta powinno być okresowo zmieniane. Hasło powinno zawierać wielkie/małe litery, znaki specjalne, cyfry o długości co najmniej 8 znaków.
3. Hasło nie powinno być przesyłane za pośrednictwem poczty elektronicznej, ponieważ może zostać przechwycone przez przestępców i wykorzystane wbrew woli Użytkownika.
4. Użytkownik nie powinien przechowywać danych niezbędnych do zalogowania w tym samym miejscu oraz nie powinien udostępniać ich osobom trzecim.
5. Użytkownik powinien unikać logowania z komputerów, do których dostęp mają również inne osoby (np. w kawiarenkach, u znajomych) jak również z tabletów i telefonów należących do osób trzecich.
6. Użytkownik powinien unikać logowania przy użyciu nieznanych jak również niezabezpieczonych i ogólnie dostępnych połączeń bezprzewodowych wi-fi, aby inne osoby nie mogły uzyskać dostępu do urządzenia Użytkownika.
7. Użytkownik nie powinien wchodzić na stronę logowania do serwisu korzystając z odnośników otrzymanych pocztą e-mail lub znajdujących się na stronach nie należących do Towarzystwa. Użytkownik powinien korzystać wyłącznie z przycisku logowania na stronie: https://inter-direct.pl/logowanie.
8. Użytkownik powinien każdorazowo sprawdzić, 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).
9. Użytkownik nie powinien odpowiadać na żadne e-maile dotyczące weryfikacji swoich danych (np. identyfikatora, hasła) lub innych ważnych informacji, ponieważ Towarzystwo nigdy nie zwraca się o podanie danych poufnych za pomocą poczty elektronicznej.

10. Użytkownik powinien 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 Użytkownika lub wystąpiło jakiekolwiek nietypowe działanie, należy bezzwłocznie skontaktować się z Towarzystwem.
11. Użytkownik powinien zwracać uwagę na stan urządzenia, za pośrednictwem którego wywołuje serwis, w szczególności:
    a) nie powinien instalować na żądanie dodatkowego oprogramowania na komputer, tablet lub telefon,
    b) powinien pamiętać, 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 urządzeniem Użytkownika przez przestępców,
    c) nie powinien otwierać podejrzanych maili i załączników, to samo dotyczy umieszczonych w wiadomościach linków. Mogą one zainfekować urządzenie Użytkownika (komputer, tablet, telefon) wirusem, d) powinien pamiętać, że 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,
    d) nie powinien udostępniać swoich urządzeń (komputer, tablet, telefon)osobom postronnym, gdyż mogą one bez wiedzy Użytkownika skopiować dane lub zainstalować/ściągnąć szkodliwe oprogramowanie, w tym wirusy.