Bezpieczne użytkowanie Panelu Administracyjnego MOBIS

1. Po zalogowaniu do Panelu Administracyjnego MOBIS nie odchodź od komputera, a po zakończeniu pracy wyloguj się i zamknij przeglądarkę.
2. Nigdy nie używaj wyszukiwarek internetowych do znalezienia strony logowania do Panelu Administracyjnego MOBIS. Zawsze wpisuj adres, który otrzymałeś w podczas szkolenia.
3. Przed zalogowaniem sprawdź, czy połączenie z Panelem Administracyjnym MOBIS jest szyfrowane, upewniając się czy adres strony logowania rozpoczyna się następująco: **https://** oraz czy na pasku przy polu adresowym pojawia się ikona z zamkniętą kłódką.
4. Nie zapisuj nigdzie haseł służących do logowania i pamiętaj o ich regularnej zmianie (zaleca się zmianę hasła po pierwszym logowaniu oraz co najmniej raz w miesiącu).
5. Sprawdzaj historię operacji wykonanych na swoim koncie.
6. Nigdy nie odpowiadaj na wiadomości e-mail, których autorzy proszą o ujawnienie lub zweryfikowanie Twoich danych osobowych, informacji dotyczących loginu konta, a także podania innych informacji o koncie administratora.

Ponadto zalecamy:

Hasło używane do logowania się w Panelu Administracyjnego MOBIS nie powinno być używane na innych stronach internetowych. Zmienianie hasła raz w miesiącu, a samo hasło powinno składać się co najmniej z ośmiu znaków będących kombinacją dużych i małych liter oraz cyfr.

Jeżeli jakikolwiek szczegół wzbudzi Państwa wątpliwość prosimy o kontakt telefoniczny z konsultantem ds. bezpieczeństwa informacji SISMS pod numerem: **+48 (71) 750-47-03** (opłata zgodna z taryfą operatora).

Bezpieczne logowanie

Przed zalogowaniem się do Panelu Administracyjnego MOBIS proszę upewnić się czy połączenie jest szyfrowane:

1. Sprawdzamy czy adres strony w oknie przeglądarki, który wpisałeś wyglądał następująco: **https://ssl.mobis.info.pl/security/login**
   Sprawdzamy czy pojawia się ikona z zamkniętą kłódką (w górnym lewym rogu okna przeglądarki). Pojawienie się kłódki sygnalizuje, że strona jest zabezpieczona certyfikatem bezpieczeństwa i połączenie jest szyfrowane.
2. Sprawdzamy poprawność certyfikatu bezpieczeństwa. Do danych certyfikatu można dotrzeć poprzez dwukrotne kliknięcie w ikonę kłódki. Po kliknięciu na zakładkę „wyświetl certyfikat”, wyświetlane są szczegóły dotyczące certyfikatu.

Jeżeli jakikolwiek szczegół wzbudzi Państwa wątpliwość prosimy o kontakt telefoniczny z konsultantem ds. bezpieczeństwa informacji SISMS pod numerem: **+48 (71) 750-47-03** (opłata zgodna z taryfą operatora).

Dobre praktyki na co dzień

Korzystanie z Internetu wiąże się z niebezpieczeństwem zainstalowania w komputerze wirusów, koni trojańskich czy programów szpiegowskich typu spyware. Wirusy to programy, które kasują i niszczą dane, rozsyłają spam, kradną dane, a w szczególności hasła, czy dane osobowe. Najprostszym sposobem uniknięcia takiego zagrożenia jest Państwa wiedza, przed czym i w jaki sposób najlepiej się zabezpieczać.

Wirusy komputerowe wykorzystują słabość zabezpieczeń komputerów podłączonych się do sieci, a także niedoświadczenie i beztroskę użytkowników Internetu. Wirusy komputerowe dostają się do komputera

najczęściej za pomocą poczty elektronicznej lub w trakcie przeglądania stron internetowych i ściągania plików z sieci. Najlepszą formą obrony przed zagrożeniami z Internetu jest zainstalowanie na komputerze dobrego programu antywirusowego z wbudowaną zaporą firewall, skanerem poczty elektronicznej, filtr antyphishingowy oraz moduł przeciwko programom spyware.

Aby zwiększyć bezpieczeństwo korzystania z Internetu, warto przestrzegać kilku ważnych zasad:

1. Z uwagi na coraz większe zagrożenie wirusami pojawiającymi się w Internecie, zalecamy przeprowadzanie częstych aktualizacji oprogramowania antywirusowego oraz częstej aktualizacji systemów operacyjnych i przeglądarek internetowych.
2. Pliki, które zapisujemy na dysk komputera przed otwarciem powinny być zawsze sprawdzone czy nie są zainfekowane przez wirusy.
3. Podczas pracy w Internecie nigdy nie wyłączamy programu antywirusowego, a także nie otwieramy „nie zaufanych” stron internetowych.