Poradnik bezpiecznego korzystania z IB

Przed zalogowaniem do serwisu i wykonaniem transakcji:

- sprawdź, czy adres strony serwisu transakcyjnego został wpisany prawidłowo: https://konto.etnobank.pl,
- sprawdź, czy na pasku adresu strony została wyświetlona zamknięta kłódka, oznaczająca nawiązanie szyfrowanego połączenia z Bankiem,
- sprawdź, czy strona serwisu jest zabezpieczona ważnym certyfikatem, którego właścicielem jest ETNO Bank Spółdzielczy,
- sprawdź, czy SMS z kodem dotyczy właściwego przelewu oraz czy numer rachunku odbiorcy i rodzaj operacji wyświetlanej w SMS i na stronie www jest zgodny z Twoją dyspozycją.

Zasady bezpiecznego dostępu i wykonywania transakcji:

- należy unikać łączenia się z publiczną siecią WiFi,
- należy zawsze korzystać z aktualnych wersji systemu operacyjnego, oprogramowania antywirusowego i przeglądarki internetowej,
- system pocztowy powinien być chroniony przed przychodzącym spamem,
- nie należy logować się do systemu korzystając z odnośników otrzymanych pocztą elektroniczną lub znajdujących się na stronach nienależących do Banku,
- należy unikać logowania z komputerów, do których dostęp mają również inne osoby,
- zalecane jest ręczne wpisywanie danych do zlecenia przelewu np. numerów rachunków, należy unikać wprowadzania numerów rachunków stosowania metody kopiuj/wklej,
- nie należy instalować oprogramowania pochodzącego z nieznanych źródeł,
- należy zawsze kończyć pracę z systemem bankowości internetowej na komputerze korzystając z polecenia – wyloguj,

Pamiętaj, że Bank nigdy nie prosi o:

- instalację certyfikatów na komputerach i telefonach komórkowych,
- podanie danych kart płatniczych i kredytowych (numer karty, kod PIN) oraz danych dotyczących Twojego telefonu (numer i model),
- udział w testowaniu nowych funkcjonalności serwisu transakcyjnego,
- wykonanie przelewów testowych ani zwrot środków na rachunki innych Klientów,

Dlaczego zabezpieczenia są tak ważne ?

Poziom bezpieczeństwa komunikacji pomiędzy witryną internetową, a jej Klientem zależy od poziomu bezpieczeństwa każdego z elementów uczestniczących w tej komunikacji. Zabezpieczenia po stronie Banku spełniają wysokie standardy i są cyklicznie testowane i audytowane. Dlatego działania cyberprzestępców ukierunkowane są na zabezpieczenia po stronie Klienta.

Bezpieczeństwo korzystania z serwisu bankowości internetowej zależy również od jego użytkowników, w tym także świadomości z obszaru zabezpieczeń własnego komputera. Niezabezpieczony komputer jest narażony na ataki z użyciem złośliwego oprogramowania, a nawet całkowite przejęcie nad nim kontroli. W takiej sytuacji cyberprzestępca, mając do dyspozycji wykradzione dane uwierzytelniające (login, hasło, SMS potwierdzający transakcję) będzie usiłował zrealizować utworzony przez siebie przelew.

W celu zachowania bezpieczeństwa środków zdeponowanych na rachunku bankowym staraj się odpowiednio zabezpieczyć komputer oraz stosuj podstawowe zasady bezpieczeństwa. Śledź na bieżąco informacje zamieszczone na stronie Banku dotyczące nowych zagrożeń w bankowości internetowej.

Przypominamy, że bezpieczeństwo transakcji realizowanych w serwisach bankowości internetowej zależy również od Ciebie oraz od zabezpieczeń, za pomocą których łączysz się z Bankiem.

W przypadku wątpliwości dotyczących bezpieczeństwa transakcji poprzez system powinieneś niezwłocznie skontaktować się z Bankiem.

Aktualne ostrzeżenia, komunikaty i poradniki dla Klientów banków publikuje również Związek Banków Polskich na stronach internetowych: http://zbp.pl/dla-konsumentów.