Zasady bezpieczeństwa w bankowości elektronicznej

Mając na uwadze bezpieczeństwo transakcji bankowych dokonywanych z wykorzystaniem Internetu tj. korzystanie przez Państwa z „Centrum Usług Internetowych", Bank Spółdzielczy w Lipnie uprzejmie prosi o zapoznanie się i stosowanie poniższych informacji i zasad. Dzięki nim, Państwa pieniądze będą jeszcze bezpieczniejsze.

Zasady ogólne:

1. Prosimy pamiętać, że żaden Bank nigdy nie wysyła do swoich klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację;
2. Komputer podłączony do Internetu musi mieć zainstalowany program antywirusowy i musi być on na bieżąco aktualizowany;
3. Płatności internetowych należy dokonywać tylko z wykorzystaniem „pewnych komputerów";
4. Na każdym komputerze winno być zainstalowane tylko legalne oprogramowanie;
5. System operacyjny i istotne dla jego funkcjonowania aplikacje np. przeglądarki internetowe, winny być systematycznie aktualizowane;
6. Prosimy nie otwierać wiadomości i dołączonych do nich załączników nieznanego pochodzenia;
7. Po zalogowaniu do systemu transakcyjnego nie należy odchodzić od komputera, a po zakończeniu pracy wylogować się i zamknąć przeglądarkę;
8. Jeśli przy logowaniu pojawią się nietypowe komunikaty lub prośby o podanie danych osobowych lub dodatkowe pola z pytaniem o hasła do autoryzacji, natychmiast prosimy zgłosić problem do naszego Banku;
9. Prosimy nie wchodzić na stronę internetową naszego Banku za pośrednictwem linków znajdujących się w przychodzących do Państwa mailach (Phishing);
10. Prosimy sprawdzać poprawność numeru NRB przed i po podpisaniu przelewu, a w szczególności po wklejeniu go ze schowka systemu. Najlepiej zrezygnować z kopiowania NRB;
11. Prosimy cyklicznie sprawdzać, czy numery rachunków w przelewach zdefiniowanych nie uległy podmianie;
12. Należy na bieżąco przeglądać historię rachunku;
13. Nie należy używać wyszukiwarek internetowych w celu znalezienia strony logowania do bankowości internetowej;
14. Przed zalogowaniem prosimy sprawdzić, czy połączenie z Bankiem jest bezpieczne (adres witryny internetowej naszego Banku powinien rozpoczynać się od skrótu: https://);
15. Prosimy sprawdzać prawidłowość certyfikatu (zanim Państwo wpiszą identyfikator i hasło, należy sprawdzić, czy połączenie z Bankiem odbywa się z wykorzystaniem szyfrowania (symbol kłódki));
16. Nie należy korzystać z bankowości elektronicznej za pośrednictwem niesprawdzonych połączeń (np. publicznej WiFi)

17. Prosimy pamiętać o nieudostępnianiu osobom trzecim identyfikatora ani hasła dostępu;
18. Hasła służące do logowania nie powinny być nigdzie zapisane i należy pamiętać o ich regularnej zmianie.

Zasady wymienione wyżej, opisane są również na stronie internetowej logowania do bankowości internetowej. Uprzejmie prosimy, o każdorazowe czytanie komunikatów wysłanych bezpośrednio tą drogą. Zawierają one ważne informacje, z którymi Państwo, w celu zwiększenia bezpieczeństwa realizowanych transakcji, powinni się zapoznać.

Informujemy również o uruchomieniu w bankowości elektronicznej usługi filtrowania adresów IP, która pozwala ograniczyć możliwość logowania tylko dla określonych adresów komputerów (np. do zakresu adresów przypisanych dostawcy Internetu). W celu zdefiniowania zakresu adresów IP należy w menu bankowości elektronicznej wybrać zakładkę ⇨Konfiguracja ⇨Filtrowanie IP, a następnie wpisać adresy IP komputerów, z których Państwo korzystają w bankowości elektronicznej*. Po skonfigurowaniu usługi, logowanie będzie możliwe tylko z komputerów posiadających adres IP ze zdefiniowanego wcześniej zakresu, co w przypadku przejęcia hasła może zabezpieczyć przed zalogowaniem się do bankowości internetowej np. z komputerów w innych krajach.

W razie jakichkolwiek pytań lub spostrzeżeń pracownicy naszego Banku pozostają do Państwa dyspozycji.

Telefon kontaktowy:

centrala Banku – (54) 237 09 00
dział IT – (54) 237 09 06

* adres IP komputera można ustalić sprawdzając w menu bankowości elektronicznej zakładkę ⇨historia logowań lub kontaktując się z dostawcą Internetu. W przypadku usługi, która nie zapewnia stałego adresu (np. Neostrada) konieczne jest wprowadzenie zakresu adresów przydzielonych danemu dostawcy.