Zasady bezpiecznego korzystania z bankowości elektronicznej

Mając na uwadze bezpieczeństwo swoich Klientów, bank Spółdzielczy w Tyczynie przedstawia praktyczny poradnik zawierający podstawowe informacje i zasady, o których warto pamiętać. Dzięki nim, Państwa pieniądze będą jeszcze bezpieczniejsze. Warto się z tymi zasadami zapoznać, warto o nich pamiętać.

1. **Bank nigdy nie wysyła do swoich klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację (uzupełnienie formularzy).**
   Bank Spółdzielczy w Tyczynie nigdy nie podaje w przesyłanych wiadomościach linków do stron transakcyjnych. Listy, wiadomości e-mail lub telefony w takich sprawach należy traktować jako próbę wyłudzenia poufnych informacji. Nie odpowiadaj na nie przekazując swoje poufne dane. Bezzwłocznie skontaktuj się z Bankiem i poinformuj o zdarzeniu.

2. **Stosuj się do procedur banku.**
   Przy każdym logowaniu bezwzględnie stosuj się do zasad bezpieczeństwa tam opublikowanych. W przypadku pojawienia się jakichkolwiek nieprawidłowości natychmiast skontaktuj się z pracownikiem Banku.

3. **Komputer / telefon komórkowy podłączony do Internetu musi mieć zainstalowany program antywirusowy i musi on być na bieżąco aktualizowany.**
   Niezbędna jest również aktywacja istotnych modułów w pakiecie ochronnym takich jak monitor antywirusowy, skaner poczty czy firewall. Częstym błędem jest wyłączanie wspomnianych modułów w celu redukcji obciążenia systemu.

4. **Nie korzystaj z bankowości elektronicznej w sieciach ogólnie dostępnych (np. darmowych).**
   Nie dokonuj płatności internetowych z komputerów znajdujących się w miejscach publicznych np. w kawiarenkach internetowych lub na uczelni.

5. **Instaluj na swoim komputerze tylko legalne oprogramowanie.**
   Programy niewiadomego pochodzenia, w tym ściągane za pośrednictwem programów typu Peer-to-Peer (P2P) mogą być przygotowane przez hakerów i zawierać wirusy lub inne szkodliwe oprogramowanie.

6. **Aktualizuj system operacyjny i istotne dla jego funkcjonowania aplikacje np. przeglądarki internetowe.**
   Hakerzy stale szukają luk w oprogramowaniu, które są następnie wykorzystywane do przestępstw internetowych. Producenci systemów operacyjnych i aplikacji publikują stosowne „łaty", których celem jest usuwanie podatności ich produktów na ataki przeprowadzane za pośrednictwem znalezionych luk. Zalecamy również okresowe wykonanie skanowania komputera programem antywirusowym, w szczególności przed wejściem na stronę internetową banku i wykonaniem jakiejkolwiek transakcji.

7. **Nie otwieraj wiadomości i dołączonych do nich załączników nieznanego pochodzenia.**
   Często załączniki takie zawierają wirusy lub inne oprogramowanie, które pozwala na szpiegowanie Twoich działań.

8. **Nigdy nie używaj wyszukiwarek internetowych do znalezienia strony logowania Banku.**
   Wyszukane w nich linki mogą prowadzić do fałszywych stron lub stron zawierających wirusy.

9. **Przed zalogowaniem sprawdź, czy połączenie z bankiem jest bezpieczne.**
   Adres witryny internetowej Banku powinien rozpoczynać się od skrótu: "https://", a nie "http://". Brak litery "s" w skrócie "http" oznacza brak szyfrowania, czyli, że Twoje dane są transmitowane przez Internet tekstem jawnym, co naraża Cię na ogromne niebezpieczeństwo.

10. **Sprawdzaj prawidłowość certyfikatu.**
    Zanim wpiszesz identyfikator bądź login i hasło sprawdź, czy połączenie z bankiem odbywa się z wykorzystaniem szyfrowania. Jeżeli znajdziesz symbol kłódki, kliknij na niego dwa razy, aby sprawdzić, czy wyświetlony certyfikat jest ważny i czy został wydany dla Banku. Jeśli certyfikat utracił ważność lub nie został wystawiony dla Banku albo nie można go zweryfikować zrezygnuj z połączenia.

11. **Nie wchodź na stronę Internetową Banku za pośrednictwem linków znajdujących się w przychodzących do Ciebie mailach (Phishing).**

    Używaj do tego celu adresu podanego Ci przez Bank, z którym podpisał(aś/eś) umowę o otwarcie i prowadzenia rachunku bankowego. Nie jest również wskazane wykorzystywanie mechanizmu „Zakładek" (Firefox) lub „adresów Ulubionych", gdyż istnieją szkodliwe obiekty, które potrafią modyfikować zachowane tam adresy.

12. **Jeśli przy logowaniu pojawią się nietypowe komunikaty** lub prośby o podanie danych osobowych lub dodatkowe pola z pytaniem o hasła do autoryzacji, natychmiast zgłoś problem do swojego Banku.

13. **Po zalogowaniu do systemu transakcyjnego nie odchodź od komputera**, a po zakończeniu pracy wyloguj się i zamknij przeglądarkę.

14. **Nigdy nie udostępniaj osobom trzecim identyfikatora ani hasła dostępu.**

    Identyfikator jest poufnym numerem nadawanym przez Bank, nie możesz go zmienić. Nie zapisuj nigdzie haseł służących do logowania i pamiętaj o ich regularnej zmianie. Idealnym rozwiązaniem jest zmienianie haseł raz w miesiącu, ale o ile system tego na Tobie nie wymusi zmieniaj je przynajmniej raz na dwa miesiące używając kombinacji dużych i małych liter oraz cyfr. Sprawdzaj datę ostatniego poprawnego oraz niepoprawnego logowania do systemu.

15. **Pracownik Banku nigdy nie kontaktuje się z Klientem z prośbą o instalację oprogramowania do zdalnego dostępu do komputera Klienta**, podanie danych dostępowych do komputera Klienta, systemów bankowych, haseł, PINów ani treści SMSów autoryzacyjnych. Oszuści podszywają się pod pracowników Banku Spółdzielczego, Zrzeszenia BPS/SGB i firm informatycznych. Cyberprzestępcy pod pozorem troski

o bezpieczeństwo Twoich środków i operacji finansowych mogą kontaktować się z Tobą telefonicznie i nakłaniać Cię do:
• przekazania identyfikatora i hasła do bankowości elektronicznej,
• podania danych kart płatniczych (numer i kod CVV/CVV2) lub innych ważnych danych (np. PESEL, skany dokumentu tożsamości),
• zainstalowania dodatkowego oprogramowania na komputer lub aplikacji na smartfonie (AnyDesk/TeamViewer),
• wyręczenia w wykonaniu lub dokończeniu transakcji w bankowości internetowej lub aplikacji mobilnej.

16. **Pamiętaj jeżeli coś wzbudza Twoje podejrzenia np. w trakcie nawiązywania sesji z bankowością internetową lub mobilną – skontaktuj się z nami.**

17. **Odwiedzaj regularnie Portal „Bezpieczny Bank" na stronie internetowej ZBP – www.zbp.pl**
    Jeśli chcesz wiedzieć więcej na temat bezpiecznego posługiwania się bankowością elektroniczną, w tym internetową regularnie odwiedzaj ten Portal. Tam fachowcy z zakresu bezpieczeństwa banku wyjaśniają jak uniknąć czyhających w sieci niebezpieczeństw.