Zasady bezpiecznego korzystania z bankowości internetowej

Przypominamy o ważnych zasadach bezpiecznego korzystania z bankowości internetowej EBP:

- Nigdy nie udostępniaj osobom trzecim swojego identyfikatora, hasła do logowania, haseł i jednorazowych narzędzi autoryzacji, danych osobowych, nr pesel, nr dowodu osobistego, nazwiska panieńskiego matki!
- Nie zapisuj nigdzie haseł ani PIN-u. Otrzymane z banku hasło lub PIN na wydruku, zapamiętaj, a następnie zniszcz!
- Nie przechowuj haseł ani narzędzi autoryzacyjnych w miejscach, w których ktoś mógłby je łatwo znaleźć, nie rób zdjęć kart kodów!
- Nie używaj tego samego hasła, którego używasz do logowania się w banku, na innych stronach internetowych, skrzynek e-mail, portali społecznościowych!
- Jeśli zmieniasz swoje hasło, wybierz takie, którego nie można łatwo odgadnąć - niech to będzie kombinacja liter i cyfr!
- Na komputerze posiadaj aktualny program antywirusowy i regularnie skanuj dyski komputera,
- Nie otwieraj wiadomości e-mail od nieznanych nadawców zawierających załączniki, np. załączone faktury, ponaglenia zapłaty, listy przewozowe!
- Sprawdzaj regularnie wyciągi bankowe, dotyczące transakcji dokonywanych kartą płatniczą.
- Nie zapisuj nr kart płatniczych w serwisach aukcyjnych, płatniczych!
- **Staraj się przy korzystaniu z bankowości elektronicznej używać własnego komputera, Zalecamy nie korzystać z bankowości elektronicznej z publicznie dostępnych sieci Wi-Fi !**
- Nigdy nie odchodź od komputera, kiedy jesteś zalogowany na swoim rachunku bankowym,
- Upewnij się, że poprawnie wylogowałeś się po zakończeniu działań na swoim rachunku poprzez opcję **"Wyloguj"!**
- W razie otrzymania podejrzanych wiadomości e-mail lub jeżeli cokolwiek wzbudzi Twój niepokój skontaktuj się telefonicznie z pracownikiem banku tel. +48 14 644 11 62!
- W razie problemów z zalogowaniem się do bankowości internetowej lub jej nieprawidłowym działaniem skontaktuj się telefonicznie z pracownikiem banku!
- Szczegółowe informacje dotyczące aktualnych zagrożeń występujących w Internecie można znaleźć na stronie:

https://zbp.pl/dla-klientow/bezpieczne-bankowanie/bankowosc-internetowa

Pamiętaj również, że Bank nigdy:

- nie prosi o podanie danych osobowych w czasie logowania do serwisu transakcyjnego (w szczególności nazwiska panieńskiego matki, numeru pesel, danych dowodu, nr karty)!
- nie wymaga podania kodu z karty kodów w czasie logowania do serwisu transakcyjnego!

- nie prosi o aktywację usług lub zwrot środków podczas logowania do serwisu transakcyjnego!
- nie wysyła na telefon komórkowy żadnych certyfikatów bezpieczeństwa lub innych aplikacji do zainstalowania!
- nie prosi o wykonanie przelewów testowych!
- nie wysyła do klientów wiadomości e-mail zawierających link do logowania do serwisu transakcyjnego.
- nie wysyła do klientów wiadomości e-mail w których prosi podanie danych o odblokowanie dostępu

Jeżeli posiadasz telefon z systemem Android bądź ostrożny podczas instalowania nowych aplikacji na telefon!

Szkodliwa aplikacja może podszywać się pod inne znane aplikacje bądź oferować nowe funkcjonalności. Pamiętaj więc, aby przede wszystkim:

- nie instalować aplikacji pobranych spoza oficjalnych sklepów, w tym poprzez linki przesłane w wiadomościach SMS, e-mail, Messenger!
- weryfikować dostępne informacje o aplikacji, np. opinie użytkowników, datę pierwszej publikacji, twórcę aplikacji, itp.!
- zwracać uwagę jakich uprawnień wymaga aplikacja – jeśli żąda uprawnień do odbierania i wysyłania SMS-ów, to istnieje ryzyko przejęcia kodów autoryzacyjnych wysyłanych przez bank!

Jeżeli Twój telefon został zainfekowany:

- natychmiast zmień hasło do systemu bankowości internetowej!
- zmień PIN do aplikacji mobilnej banku!
- **przywróć ustawienia fabryczne w telefonie!**

"Uwaga na złośliwe oprogramowanie GozNym.

Wirus instaluje się poprzez załączniki w wiadomościach e-mail na komputerze klienta i blokuje połączenie ze stroną bankowości internetowej Banku. Klient przekierowywany jest na fałszywą stronę, ale wyglądającą identycznie jak prawdziwa strona Banku. Następnie po podaniu loginu i hasła klient proszony jest o podanie kodu jednorazowego. Tym samym dane logowania klient zdradza przestępcom. Prosimy o zachowanie ostrożności. Bank nigdy nie przesyła żadnych informacji na temat logowania w wiadomościach mailowych do użytkowników. Każda taka wiadomość przesłana w mailu wygenerowana została przez przestępców. W przypadku jakichkolwiek wątpliwości prosimy o kontakt z pracownikami Banku."