BEZPIECZEŃSTWO KORZYSTANIA Z BANKOWOŚCI INTERNETOWEJ

Zadbaj o swoje bezpieczeństwo w internecie

Aby bezpiecznie korzystać z bankowości internetowej:

- należy posiadać legalne oprogramowanie,
- należy na bieżąco aktualizować system operacyjny (Windows) oraz szczególnie narażone na ataki hakerskie oprogramowania, takie jak: przeglądarki internetowe, java, flash player oraz oprogramowanie do obsługi plików pdf,
- należy posiadać ochronę antywirusową z aktualną bazą wirusów,
- zawsze przed logowaniem należy sprawdzić, czy adres strony banku rozpoczyna się od

https://ebanknet.bs-warta.pl/,

-

należy zawsze przed logowaniem zweryfikować Certyfikat Bezpieczeństwa Banku, którego szczegóły są dostępne poprzez kliknięcie na symbol kłódki w oknie przeglądarki,

-

należy unikać przeklejania numerów rachunków, zalecane jest ręczne wpisywanie do zleceń w systemie bankowości internetowej albo o uważną kontrolę wklejanego numeru rachunku i porównanie tego numeru z oryginalnym, kopiowanym numerem rachunku,

-

należy unikać logowania z komputerów, do których dostęp mają również inne osoby (np. w kawiarenkach, u znajomych),

-

należy zawsze kończyć pracę korzystając z polecenia – Wyloguj,

-

nie należy przesyłać mailem żadnych danych osobistych typu hasła, numery kart itp.,

-

nie należy wchodzić na stronę logowania do systemu korzystając z odnośników otrzymanych pocztą e-mail lub znajdujących się na stronach nie należących do banku,

-

nie należy odpowiadać na żadne e-maile dotyczące weryfikacji Twoich danych (np. identyfikatora, hasła) lub innych ważnych informacji – bank nigdy nie zwraca się o podanie danych poufnych za pomocą poczty elektronicznej,

-

nie należy przechowywać nazwy użytkownika i haseł w tym samym miejscu oraz udostępniać ich innym osobom.

W przypadku wątpliwości co do prawidłowości działania bankowości internetowej,

należy niezwłocznie skontaktować się z Bankiem.

RADY PRZYDATNE DLA ZACHOWANIA BEZPIECZEŃSTWA PODCZAS DOKONYWANIA TRANSAKCJI PŁATNICZYCH

1. Podczas transakcji nie należy tracić karty z pola widzenia. Po transakcji należy ją odebrać bez zbędnej zwłoki.

2. Należy zachować rozwagę przy przekazywaniu numeru karty. Nie należy udostępniać numeru karty nikomu, kto do nas dzwoni, również w sytuacji, gdy osoba dzwoniąca informuje, że są problemy z komputerem i proszą o weryfikację informacji. Nie ma zwyczaju by firmy dzwoniły prosząc przez telefon o numer karty kredytowej. Jeżeli to my inicjujemy połączenie,

również nie należy udostępniać numeru karty przez telefon, gdy nie mamy pewności, że rozmówca zasługuje na zaufanie.

3. Nigdy nie odpowiadaj na pocztę elektroniczną, z której wynika konieczność podania informacji o karcie. Nigdy też nie odpowiadaj na maile które zapraszają do odwiedzenia strony internetowej w celu weryfikacji danych, w tym o kartach. Ten rodzaj oszustwa jest nazywanych „phishingiem".

4. Nigdy nie należy podawać informacji o karcie na stronach, które nie są bezpieczne. Np. strony ze zdjęciami pornograficznymi lub strony nieznanych szerzej firm oferujące markowy towar po rewelacyjnych cenach ?

5. Kartę należy podpisać natychmiast po jej otrzymaniu.

6. Niszcz przed ewentualnym wyrzuceniem wszystkie wnioski na karty kredytowe, które możesz otrzymać drogą pocztową.

7. Nie zapisuj kodu PIN na karcie, ani nie przechowuj go razem z kartą (na wypadek kradzieży portfela czy portmonetki).

8. Nigdy nie zostawiaj karty ani pokwitowań transakcji bez nadzoru.

9. Chroń swój numer karty i inne poufne kody umożliwiające dokonane transakcji (np. numer PIN, numer CVV 2, numer CVC2), by obcy nie mogli wejść w jego posiadanie, rejestrując obraz karty np. przy użyciu telefonu komórkowego z aparatem fotograficznych, kamerą video lub w inny sposób.

10. Sporządź i przechowuj w bezpiecznym miejscu listę numerów kart oraz adresów i telefonów do każdego banku, którego karty posiadasz. Listę tą należy aktualizować za każdym razem, gdy otrzymujemy nowa kartę.

11. Należy ze sobą nosić tylko te karty, które się potrzebuje. Nie należy nosić ze sobą kart, z których się rzadko korzysta.

12. Traktuj transakcje kartowe z podobna rozwagą jak inne dokonane na rachunku. Sprawdzaj wykonane operacje niezwłocznie po otrzymaniu wyciągu rachunku dla kart debetowych i zestawienia transakcji dla pozostałych kart. Zachowanie pokwitowań dokonanych transakcji pozwala na szybką ich weryfikację.

13. Zawsze niszcz nieprawidłowe pokwitowania, zbieraj pokwitowania transakcji, które nie doszły do skutku

14. Przed wyrzuceniem niszcz wszystkie dokumenty, które zawierają pełen numer karty.

15. W restauracjach, gdy otrzymujesz wydruk z terminala z miejscem na wpisanie napiwku wpisz kwotę, lub przekreśl to miejsce poziomą kreską.

16. Nigdy nie zapisuj numeru karty w miejscu publicznie dostępnym (np. na pocztówce).

17. Dobrym pomysłem jest noszenie kart poza portfelem, najlepiej w oddzielnej zamykanej

przegródce lub etui.

18. Nigdy nikomu nie udostępniaj kart.

19. Jeśli się przeprowadzasz, nie zapomnij jak najszybciej poinformować banku, który wydał karty, o zmianie adresu.

20. Nie zabieraj karty ze sobą, jeżeli jej użycie jest mało prawdopodobne, a możesz narazić się na jej utratę (np. zakupy na bazarach i w miejscach gdzie możesz być narażony na kradzież kieszonkową).

21. Jeżeli byłeś w sytuacji, która sprzyja kradzieży sprawdź czy masz karty (np. w przedziale pociągu, gdy rozpoczynasz podróż).