Kodeks Bezpieczeństwa

mBank

mBank.pl

Spis treści

W Kodeksie Bezpieczeństwa, znajdziesz wskazówki, jak bezpiecznie korzystać z bankowości internetowej i mobilnej oraz jak chronić się przed zagrożeniami ze strony cyberprzestępców.

Urządzenie

1. Z serwisów banku korzystaj tylko na sprawdzonych urządzeniach. Unikaj logowania z cudzych komputerów i urządzeń mobilnych.
2. Korzystaj z dodatkowych programów (np. antywirus, firewall), które chronią komputery i urządzenia mobilne.
3. Regularnie aktualizuj system operacyjny na Twoim komputerze.
4. Nie zmieniaj samodzielnie konfiguracji bezpieczeństwa urządzenia, a w szczególności nie usuwaj ograniczeń, które narzucił producent.
5. Aplikacje i programy pobieraj wyłącznie z oficjalnych źródeł.
6. Włącz ustawienia blokady ekranu Twojego urządzenia (np. hasło, PIN).

Hasła

7. Stosuj skomplikowane hasła. Zadbaj o to, aby trudno było je odgadnąć (minimum osiem znaków, w tym znaki specjalne, liczby, duże i małe litery).
8. Nie używaj w haśle trywialnych zwrotów oraz informacji, które łatwo z Toba powiązać (np. imię czy nazwisko) lub odgadnąć (np. aktualny miesiąc, rok).
9. Regularnie zmieniaj hasła i nie udostępniaj ich nikomu.
10. Używaj unikalnych haseł do serwisów banku. Nie wykorzystuj tych samych haseł, które stosujesz w innych systemach bankowych, na forach, czy portalach.

Strony www

11. Sprawdzaj poprawność witryny serwisu bankowego, z którym się łączysz (certyfikat oraz połączenie HTTPS).
12. Nie wchodź na podejrzane i nieznane witryny - zwracaj uwagę na adresy URL stron, które odwiedzasz, zwłaszcza na tzw. skrócone adresy URL, np. http://bit.ly/2GeFeLg. Takie strony mogą zainfekować Twoje urządzenie złośliwym oprogramowaniem.
13. Nie podawaj danych osobowych na niezaufanych witrynach, w szczególności nigdy nie podawaj swojego loginu i hasła bankowego na stronach obcych serwisów.
14. Logując się do banku lub stron integratora płatności, zawsze samodzielnie wpisuj stronę logowania lub używaj przycisku „Zaloguj” po ręcznym wpisaniu adresu strony. Nigdy:
    - nie korzystaj z linków do logowania, które otrzymujesz mailem, w portalach społecznościowych
    - nie szukaj strony do logowania w wyszukiwarce internetowej – możesz trafić na fałszywe strony, które udają stronę Twojego banku

Maile

15. Nie otwieraj podejrzanych maili i załączników.
16. Zwracaj szczególną uwagę na załączniki posiadające kilka rozszerzeń plików jednocześnie, np. przelew.pdf.zip, wyplata.jar.doc.
17. Sprawdzaj, czy rzeczywisty adres odnośnika (link) jest spójny z tym, który widzisz w treści maila (zweryfikuj poprzez przesunięcie kursora na ten link i podświetlenie adresu).
18. Zwracaj uwagę na wiarygodność nadawcy oraz sposób w jaki zwraca się do Ciebie.
19. Nigdy nie loguj się do banku z linka, który otrzymałeś w mailu.
20. Nie realizuj transakcji na podstawie maila. Sprawdź dokładnie tego typu dyspozycje.

Portale i oferty internetowe

21. Jeżeli dostałeś prośbę od znajomego o przelew, uważaj – możliwe, że piszesz z oszustem. Skontaktuj się ze znajomym w inny sposób i potwierdź, że faktycznie to on prosi Cię o przelew.
22. Przed zakupem sprawdź, od kogo kupujesz towar: jak długo istnieje dana firma, gdzie ma siedzibę, czy możesz dodzwonić się na infolinię sklepu, czy odpisują na maile oraz jakie opinie wystawili inni kupujący. Upewnij się, czy możesz zapłacić przez integratora płatności.
23. Nie ufaj ofertom pracy, które otrzymujesz bezpośrednio na Twoją skrzynkę pocztową, szczególnie tym wyjątkowo „atrakcyjnym". Nie daj się nabrać na oferty pośrednika finansowego, które mogą okazać się przestępstwem. Gdy szukasz pracy, korzystaj wyłącznie ze znanych portali.

Rozmowy telefoniczne

24. Nie ujawniaj prywatnych danych, dopóki nie upewnisz się, z kim rozmawiasz. Pracownika banku zawsze możesz zweryfikować oddzwaniając na mLinię i potwierdzając jego tożsamość.
25. Nie ufaj nieznanemu rozmówcy, który chce, abyś podał poufne dane (w szczególności hasła, numery kart płatniczych, PINy), np. pod pretekstem:
    - rozpracowywania grupy przestępczej (tzw. metoda „na policjanta") lub
    - sprawdzenia konta, potwierdzenia przelewu czy zwrotu środków (tzw. metoda „na pracownika banku")

Policjant/pracownik banku nigdy nie poproszą Cię o Twoje poufne dane do konta.

Karty

26. Zanim skorzystasz z bankomatu, zwróć uwagę czy na urządzeniu nie ma obco wyglądających listw, nakładek lub pojemników na ulotki reklamowe. Dodatkowo, przyjrzyj się szczelinie czytnika, do którego wkładasz kartę – tam przestępcy mogą założyć tzw. skimmery, czyli nakładki „czytające" karty. Klawiatura urządzenia powinna być płaska, bez wyraźnie odstających elementów.

27. Gdy wprowadzasz PIN, koniecznie zasłoń klawiaturę drugą ręką (na wypadek gdyby przestępca zainstalował mikrokamerę skierowaną na klawiaturę).
28. Jeśli coś budzi Twój niepokój, przerwij transakcję i spokojnie odejdź od urządzenia. Następnie zadzwoń do właściciela bankomatu (numer telefonu znajduje się na każdym urządzeniu).
29. Gdy płacisz w punkcie handlowo-usługowym, pod żadnym pozorem nie trać karty z oczu (nawet jeśli znasz i lubisz daną restaurację). Pracownik punktu powinien podejść do Ciebie z terminalem.
30. Gdy płacisz kartą w internecie, upewnij się, że:
    - połączenie z witryną jest bezpieczne - adres strony internetowej zaczyna się od „https://"
    - wpisany adres jest poprawny
    - strona posiada ważny certyfikat (w górnym oknie przeglądarki powinna znajdować się mała ikona z kłódką)

Komunikaty

31. Uważnie czytaj powiadomienia Mobilnej autoryzacji oraz komunikaty SMS, w tym potwierdzenia transakcji. Treść (rodzaj operacji, numer rachunku i kwota) muszą zgadzać się z tym, co zleciłeś w serwisie transakcyjnym.
32. Uważnie czytaj ostrzeżenia mBanku przed nowymi zagrożeniami i stosuj się do zaleceń.
33. Jeżeli otrzymałeś od operatora telekomunikacyjnego komunikat o wydaniu duplikatu karty SIM, którego nie zamawiałeś, natychmiast zadzwoń do konsultanta mLinii lub Eksperta Online.

Usługi

34. Korzystaj z Mobilnej autoryzacji - nowej bezpiecznej metody potwierdzania operacji, opartej o aplikację mobilną mBanku.
35. Włącz Wyciągi szyfrowane - usługę dostarczania przez mBank wyciągów w formie zaszyfrowanej, dzięki czemu informacje zawarte w twoich wyciągach do rachunków i kart kredytowych będą jeszcze bezpieczniejsze.

Pamiętaj!

Dane to dzisiaj twarda waluta i w wyniku prostych ataków socjotechnicznych można je wykorzystać do wyprowadzenia pieniędzy z konta. Włącz szyfrowanie wyciągów, stosuj silne hasła nie tylko do bankowości, ale do wszystkich serwisów w których znajdują się Twoje dane, szczególnie te wrażliwe. Przed wpisaniem swoich danych do formularza zastanów się, jak się na nim znalazłeś i jaki jest zakres danych, które masz podać. Być może jesteś na stronie przygotowanej przez przestępców. Jeśli jakikolwiek komunikat, wiadomość od nas czy element serwisu transakcyjnego lub mobilnego budzą Twoje wątpliwości – przerwij czynność i natychmiast zadzwoń do konsultanta mLinii lub Eksperta Online.