JAK BEZPIECZNIE KORZYSTAĆ

z bankowości internetowej
EBO eBANK Online

DROGI KLIENCIE!

Nasz bank przywiązuje dużą uwagę do kwestii bezpieczeństwa, stosując najnowocześniejsze zabezpieczenia sprzętowe i programowe, by chronić Twoje dane i środki zgromadzone na koncie.

Jednak nawet najsilniejsze mechanizmy nie są w stanie zapobiec oszustwom, gdy sam udostępnisz oszustom swoje dane logowania.

PAMIĘTAJ, ŻE ŻADEN PRACOWNIK NASZEGO BANKU NIGDY NIE POPROSI CIĘ O DANE DO LOGOWANIA – ANI PRZEZ TELEFON, ANI E-MAIL, ANI SMS.

Cyberprzestępcy mają wiele sposobów, by wyłudzić wrażliwe informacje, podszywając się pod zaufane instytucje lub wzbudzając zaufanie. Poznaj najczęstsze metody, które stosują oszuści.

CO ZROBIĆ, BY TWOJE KONTO BANKOWE I ZGROMADZONE NA NIM OSZCZĘDNOŚCI BYŁY BEZPIECZNE?

1. Nie udostępniaj swoich danych.

Nigdy nie podawaj loginu, hasła, numeru PESEL, numeru telefonu, adresu e-mail, danych karty ani kodu BLIK osobom trzecim, nawet jeśli podają się za pracowników banku. **Bank nigdy nie poprosi Cię o te informacje przez SMS, e-mail, czy telefon.**

2. Korzystaj tylko z bezpośrednich linków do strony banku.

Nie wchodź na stronę internetową banku za pośrednictwem linków znajdujących się w przychodzących do Ciebie wiadomościach e-mail, SMS oraz komunikatorach (np. WhatsApp, Messenger). Mogą one prowadzić do fałszywych stron, które podszywają się pod stronę banku.

3. Nie otwieraj wiadomości nieznanego pochodzenia i dołączonych do nich załączników.

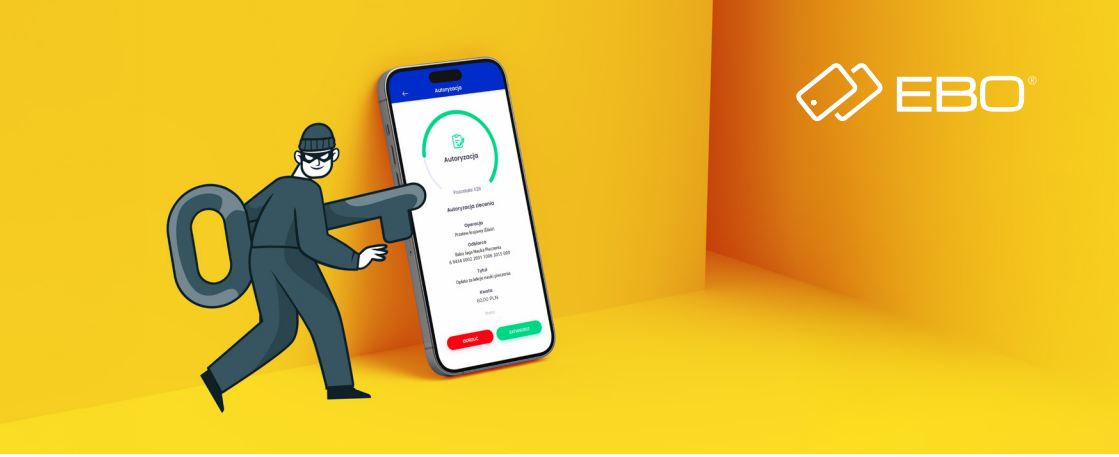
Wiadomości od nieznanych nadawców mogą zawierać wirusy lub inne złośliwe oprogramowanie, które pozwala na szpiegowanie Twoich działań w Internecie.

4. Unikaj logowania do banku w publicznych sieciach Wi-Fi.

Logowanie się do bankowości internetowej w niezabezpieczonych sieciach Wi-Fi, np. w kawiarniach, hotelach czy galeriach, naraża Cię na ataki hakerskie. Korzystaj tylko z zaufanych i zabezpieczonych sieci lub użyj VPN.

5. Sprawdzaj autentyczność strony internetowej banku.

Zawsze upewnij się, że adres strony zaczyna się od „https://" i widoczna jest zamknięta kłódka. Kliknij dwukrotnie na ikonę kłódki, aby sprawdzić, czy wyświetlony certyfikat jest ważny i czy został wydany dla naszego banku.



6. Korzystaj z bezpiecznego logowania.

Wybieraj logowanie dwuetapowe – dzięki dodatkowym kodom SMS, aplikacji uwierzytelniającej Twoje konto jest lepiej zabezpieczone przed nieuprawnionym dostępem, nawet jeśli ktoś zdobędzie Twoje hasło. Rozważ użycie klucza uwierzytelniającego U2F (Universal 2nd Factor) jako dodatkowego sposobu logowania, który uniemożliwia nieautoryzowany dostęp, nawet gdy ktoś uzyska Twoje hasło.

7. Bądź czujny podczas korzystania z bankowości internetowej.

Po zalogowaniu do bankowości internetowej nie odchodź od komputera, a po zakończeniu pracy wyloguj się z systemu i zamknij przeglądarkę, aby zapobiec nieautoryzowanemu dostępowi.

8. Twórz silne i unikalne hasła.

Hasła powinny składać się z cyfr, wielkich i małych liter oraz znaków specjalnych. Nie zapisuj haseł na kartkach ani w plikach na komputerze i nie używaj tego samego hasła do różnych kont.

9. Zarządzaj limitami operacji.

Ustal limity transakcji w bankowości internetowej oraz dla płatności kartą w Internecie. Dzięki temu, żadna transakcja przekraczająca ustalony limit nie zostanie zrealizowana bez Twojej zgody.

10. Regularnie aktualizuj systemy i przeglądarki internetowe.

Aktualizacje zawierają tzw. „łaty”, których celem jest usuwanie podatności systemu czy aplikacji na ataki przeprowadzane z wykorzystaniem luk bezpieczeństwa. Na każdym komputerze, tablecie, telefonie z dostępem do Internetu wgraj program antywirusowy.

NAJCZĘSTSZE METODY, JAKIMI POSŁUGUJĄ SIĘ OSZUŚCI:

Phishing – oszustwo, które polega na podszywaniu się pod zaufane instytucje, np. banki czy urzędy. Cyberprzestępcy wysyłają e-maile lub SMS-y z linkami do fałszywych stron internetowych, gdzie próbują wyłudzić Twoje dane logowania, numery kart lub inne wrażliwe informacje.

Vishing (voice phishing) – atak polegający na kontakcie telefonicznym. Oszuści, podszywając się pod pracowników banku lub innych instytucji, nakłaniają do podania danych osobowych lub wykonania przelewu.

Smishing – metoda, która polega na wysyłaniu fałszywych SMS-ów zawierających linki do stron phishingowych lub wyłudzających dane logowania.

Skimming – metoda polegająca na kopiowaniu danych z paska magnetycznego karty bankowej. Przestępcy wykorzystują specjalne urządzenia montowane np. w bankomatach lub terminalach płatniczych, by skopiować dane karty, które następnie mogą zostać użyte do nieautoryzowanych transakcji.

Oszustwo na BLIK – przestępcy wykorzystują komunikatory internetowe, podszywając się pod znajomych lub rodzinę, prosząc o podanie kodu BLIK do „pilnej" płatności. Często przybierają różne preteksty, np. nagły wypadek lub problem z dostępem do własnych środków.

SPAM – masowe wysyłanie niechcianych wiadomości e-mail lub SMS zawierających linki do niebezpiecznych stron lub próbujące nakłonić do podjęcia określonych działań, takich jak kliknięcie linku lub otwarcie załącznika. SPAM może zawierać zarówno phishing, jak i złośliwe oprogramowanie.

Malware – złośliwe oprogramowanie instalowane na urządzeniu użytkownika podczas pobierania aplikacji spoza oficjalnych sklepów lub otwierania załączników z nieznanych źródeł. Może przechwytywać dane logowania i inne poufne informacje.

Fałszywe aplikacje – aplikacje podszywające się pod oprogramowanie bankowe lub inne popularne aplikacje, które wyłudzają dane logowania. Pobieraj aplikacje tylko z oficjalnych źródeł, sprawdzając nazwę wydawcy.