Załącznik nr 3
do zarządzenia Członka Zarządu Banku Pani Magdaleny Falkowskiej
nr 05/02/2026 z dnia 13 lutego 2026 roku

BANK NOWY S.A.

Tabela informacyjna

Obowiązuje od dnia 17 lutego 2026 r.

Spis treści

I. Informacje ogólne

1. Niniejszy dokument stanowi Tabelę informacyjną, o której mowa w:
   - Regulaminie otwierania i prowadzenia Kont dla klientów indywidualnych;
   - Regulaminie korzystania z bankowości elektronicznej bankNOWY24;
   - Regulaminie wydawania i używania kart płatniczych dla klientów indywidualnych;
   - Regulaminie świadczenia usług płatniczych dla klientów indywidualnych;
   - Regulaminie korzystania z usługi nowySMS.
2. Tabela informacyjna stanowi zbiór informacji dotyczących oferty Banku w zakresie Kont dla klientów indywidualnych, usług bankowości elektronicznej oraz kart płatniczych, a także wytycznych w obszarze bezpieczeństwa transakcji i instrumentów płatniczych oraz obowiązków, jakie na Ciebie nakładamy w związku z korzystaniem z nich.

II. Oferta dla Klientów Indywidualnych

1. Konta – podstawowe informacje

Nazwa	noweKONTO OSOBISTE	noweKONTO DEPOZYTOWE	noweKONTO PROFIT	Podstawowy rachunek płatniczy
Typ rachunku	Rachunek oszczędnościowo – rozliczeniowy	Rachunek oszczędnościowo – rozliczeniowy	Rachunek oszczędnościowy	Rachunek oszczędnościowo – rozliczeniowy
Tryb zawarcia umowy	pisemnie w placówce	– elektronicznie przez elektroniczny formularz na stronie https://banknowy.pl/ – pisemnie w placówce	pisemnie w placówce	pisemnie w placówce
Okres umowny	Czas nieokreślony	Czas nieokreślony	Czas nieokreślony	12 miesięcy
Kto może być posiadaczem	– Osoba fizyczna posiadająca pełną zdolność do czynności prawnych, – szkolna kasa oszczędnościowa, – pracownicza kasa zapomogowo-pożyczkowa	Osoba fizyczna posiadająca pełną zdolność do czynności prawnych	Osoba fizyczna posiadająca pełną zdolność do czynności prawnych	Osoba fizyczna posiadająca pełną zdolność do czynności prawnych
Możliwość otworzenia Konta jako wspólne	tak	nie	tak	nie
Liczba rachunków jaką można otworzyć	– 1 konto indywidualne – 1 konto wspólne	1 konto indywidualne	– 1 konto indywidualne – 1 konto wspólne	1 konto indywidualne
Dostęp do rachunku za pomocą Infolinii Banku	nie	nie	nie	nie

Tabela informacyjna

Godziny pracy Infolinii	pn-pt 9:00-13:00 (obsługa rachunków)
Numery telefonu Infolinii	13 46 55 750 801 372 772

2. Bankowość elektroniczna

1) Specyfikacja techniczna sprzętu i oprogramowania niezbędna oraz zalecana do prawidłowego korzystania z bankNOWY24.

Bank zaleca korzystanie z:

- przeglądarki internetowej w najnowszej dostępnej wersji, np. Firefox, Edge, Chrome, Opera, Brave, Safari,
- legalnej wersji systemu operacyjnego z zainstalowanymi wszystkimi dostępnymi aktualizacjami systemu,
- oprogramowania antywirusowego z aktualną bazą zagrożeń/wirusów.

2) Możliwość złożenia wniosku o Produkt lub zawarcia umowy o Produkt za pośrednictwem bankNOWY24

Nazwa	noweKONTO OSOBISTE	noweKONTO DEPOZYTOWE	noweKONTO PROFIT	Podstawowy rachunek płatniczy
Możliwość złożenia wniosku o Produkt	tak	nie	tak	nie
Możliwość zawarcia umowy o Produkt	tak	nie	tak	nie

3) Zastrzeganie bankNOWY24

a. W jakiej sytuacji należy zablokować dostęp?

i. wystąpienia na rachunku nieznanych operacji,

ii. otrzymania wiadomości SMS z kodem autoryzacyjnym pomimo nie dokonywania żadnych operacji,
iii. utraty środków na rachunku,
iv. podejrzenia posiadania danych do logowania do bankowości elektronicznej przez osoby trzecie

b. Jak zablokować dostęp?
   i. W celu zablokowania dostępu do bankowości elektronicznej bankNOWY24 należy:
      a) Wejść na stronę logowania do serwisu - www.banknowy24.pl,
      b) Wybrać opcję "Zablokuj dostęp",
      c) Wprowadzić numer login, który ma zostać zablokowany,
      d) Wprowadzić ostatnio używane hasło do logowania,
      e) Wybrać przycisk "Zablokuj",
      f) Zweryfikować czy wyświetlony komunikat potwierdza zablokowanie dostępu do serwisu.
   ii. Zablokowanie dostępu jest bezpłatne. Po zablokowaniu dostępu należy poinformować o tym fakcie Bank Nowy S.A. za pośrednictwem jednego z niżej wymienionych kanałów komunikacji:
      a) wiadomości e-mail wysłanej na adres: online@banknowy.pl,
      b) formularza kontaktowego dostępnego na stronach Banku Nowego S.A.: www.banknowy.pl
      c) w placówce Banku.

4) Certyfikaty bezpieczeństwa wystawione dla Banku na stronach internetowych; sposoby weryfikacji certyfikatu

Każda strona internetowa w domenie banknowy.pl posiada stosowny certyfikat SSL. Przed zalogowaniem się do bankowości elektronicznej należy zweryfikować certyfikat oraz adres strony. W tym celu należy:

a. Sprawdzić czy strona, na której się znajdujesz, to https://www.banknowy24.pl/ebank/start Upewnij się, że strona rozpoczyna się od https. Początek adresu “https” oznacza, że strona używa szyfrowania SSL.
b. Wyświetlić informacje o certyfikacie Banku Nowego – naciśnij ikonę kłódki na pasku adresu i otwórz informacje o certyfikacie. Możesz również kliknąć ikonę informacji o witrynie

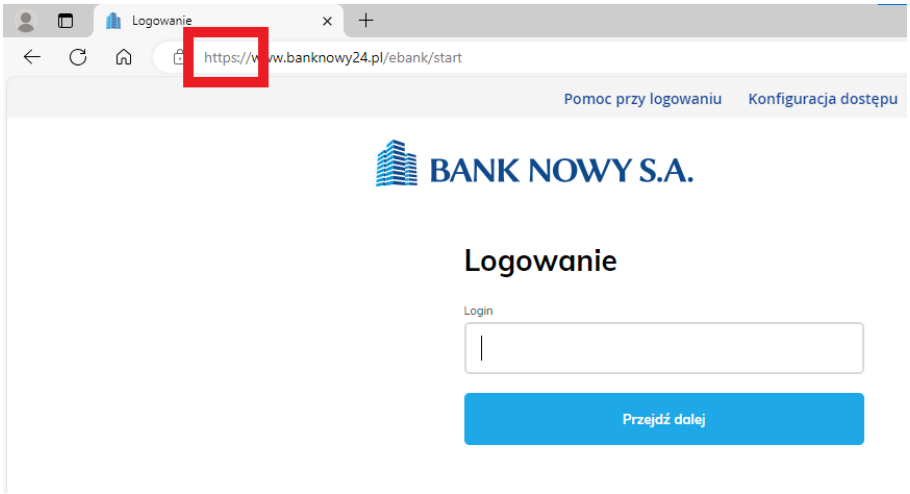
(zwykle “i” lub ikona kłódki) po lewej stronie paska adresu, a następnie kliknąć “Certyfikat” lub “Wyświetl certyfikat”.

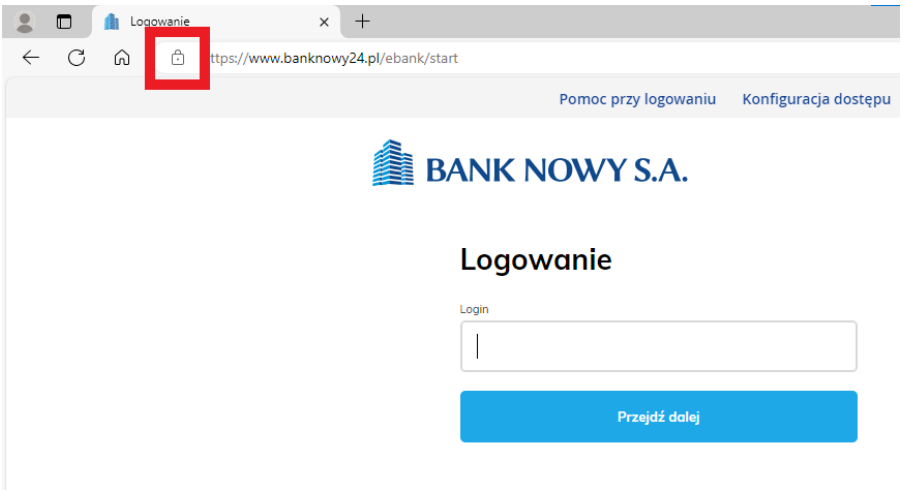
c. Zweryfikować szczegóły certyfikatu - okno informacji o certyfikacie wyświetla różne szczegóły dotyczące certyfikatu SSL. Sprawdź, czy certyfikat został wystawiony dla „Bank Nowy S.A.”. Jeśli nazwa domeny nie pasuje, certyfikat SSL może być fałszywy i nie powinieneś kontynuować logowania.

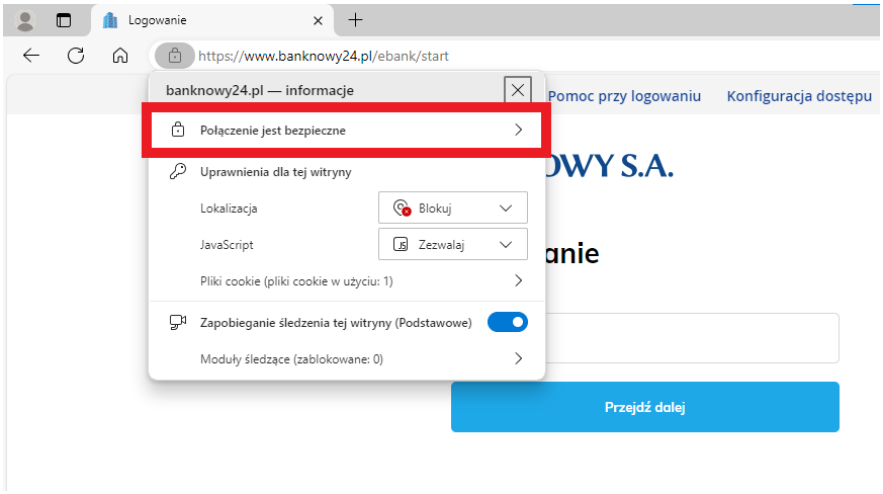
d. Sprawdzić ważność certyfikatu SSL - upewnij się, że aktualna data przypada pomiędzy datą wystawienia i datą wygaśnięcia. Jeśli certyfikat wygasł lub nie jest jeszcze ważny, przeglądarka może wyświetlić ostrzeżenie lub zablokować dostęp do witryny.

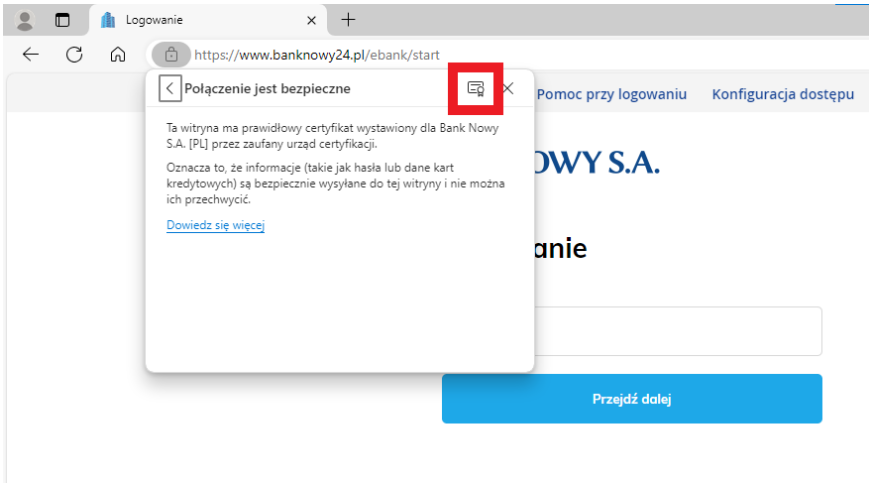
e. Sprawdzić organ wydający certyfikat - sprawdź kto jest wystawcą certyfikatu SSL lub Certificate Authority (CA). Urząd certyfikacji powinien być renomowaną i zaufaną organizacją, taką jak **Digicert**, Symantec lub Comodo. Jeśli wystawca jest nieznany lub niezaufany, może to być oznaką fałszywego certyfikatu SSL

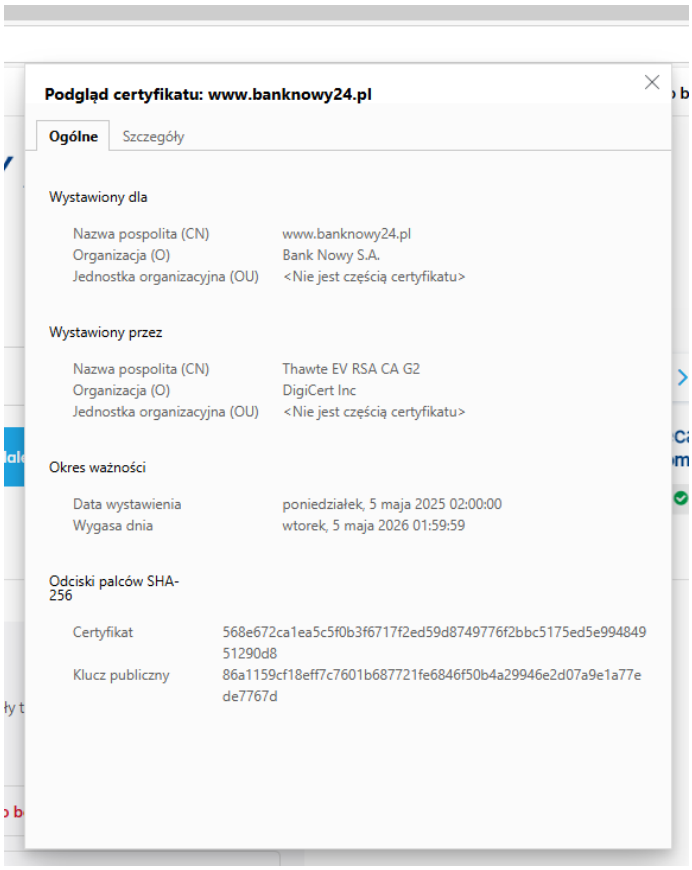
Na poniższych zrzutach ekranu przedstawiono krok po kroku, w jaki sposób należy zweryfikować certyfikat oraz adres strony. Weryfikację certyfikatu wykonano na przykładzie przeglądarki Microsoft Edge.

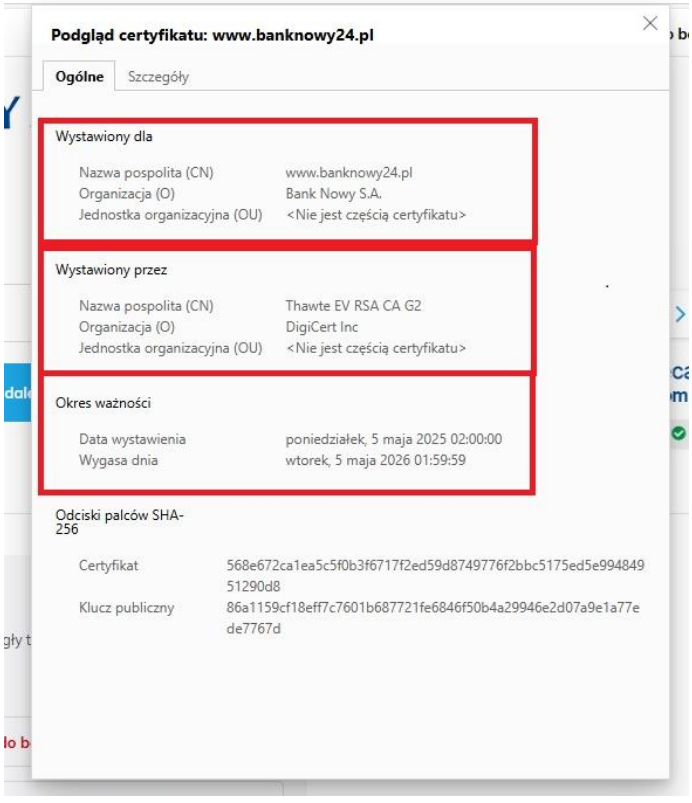



Logowanie
https://www.banknowy24.pl/ebank/start
Pomoc przy logowaniu
Konfiguracja dostępu
BANK NOWY S.A.
Logowanie
Login
Przejdź dalej


Logowanie
https://www.banknowy24.pl/ebank/start
banknowy24.pl — informacje
Połączenie jest bezpieczne
Uprawnienia dla tej witryny
Lokalizacja
Blokuj
JavaScript
Zezwalaj
Pliki cookie (pliki cookie w użyciu: 1)
Zapobieganie śledzenia tej witryny (Podstawowe)
Moduły śledzące (zablokowane: 0)
Pomoc przy logowaniu
Konfiguracja dostępu
Przejdź dalej


Logowanie
https://www.banknowy24.pl/ebank/start
Połączenie jest bezpieczne
Ta witryna ma prawidłowy certyfikat wystawiony dla Bank Nowy S.A. [PL] przez zaufany urząd certyfikacji.
Oznacza to, że informacje (takie jak hasła lub dane kart kredytowych) są bezpiecznie wysyłane do tej witryny i nie można ich przechwycić.
Dowiedz się więcej
Pomoc przy logowaniu
Konfiguracja dostępu
Przejdź dalej


Podgląd certyfikatu: www.banknowy24.pl
Ogólne
Szczegóły
Wystawiony dla
Nazwa pospolita (CN) www.banknowy24.pl
Organizacja (O) Bank Nowy S.A.
Jednostka organizacyjna (OU) <Nie jest częścią certyfikatu>
Wystawiony przez
Nazwa pospolita (CN) Thawte EV RSA CA G2
Organizacja (O) DigiCert Inc
Jednostka organizacyjna (OU) <Nie jest częścią certyfikatu>
Okres ważności
Data wystawienia poniedziałek, 5 maja 2025 02:00:00
Wygasa dnia wtorek, 5 maja 2026 01:59:59
Odciski palców SHA-256
Certyfikat 568e672ca1ea5c5f0b3f6717f2ed59d8749776f2bbc5175ed5e99484951290d8
Klucz publiczny 86a1159cf18eff7c7601b687721fe6846f50b4a29946e2d07a9e1a77ede7767d


Podgląd certyfikatu: www.banknowy24.pl
Ogólne
Szczegóły
Wystawiony dla
Nazwa pospolita (CN) www.banknowy24.pl
Organizacja (O) Bank Nowy S.A.
Jednostka organizacyjna (OU) <Nie jest częścią certyfikatu>
Wystawiony przez
Nazwa pospolita (CN) Thawte EV RSA CA G2
Organizacja (O) DigiCert Inc
Jednostka organizacyjna (OU) <Nie jest częścią certyfikatu>
Okres ważności
Data wystawienia poniedziałek, 5 maja 2025 02:00:00
Wygasa dnia wtorek, 5 maja 2026 01:59:59
Odciski palców SHA-256
Certyfikat 568e672ca1ea5c5f0b3f6717f2ed59d8749776f2bbc5175ed5e99484951290d8
Klucz publiczny 86a1159cf18eff7c7601b687721fe6846f50b4a29946e2d07a9e1a77ede7767d

5) Aktualne ostrzeżenia i rekomendacje Banku, w zakresie bezpieczeństwa korzystania z bankNOWY24 oraz wykonywania za jej pośrednictwem Transakcji płatniczych, publikowane są na stronie internetowej Banku. Poniżej przedstawiono ostrzeżenia dotyczące najczęściej występujących oszustw oraz rekomendacje w zakresie bezpieczeństwa.

a. Rekomendacje Banku w zakresie bezpieczeństwa

i. Należy kierować się zasadą ograniczonego zaufania! - nigdy nie masz pewności, kto znajduje się po "drugiej stronie", a bycie podejrzliwym to dla Ciebie najlepsza ochrona!

ii. Logowania do bankowości elektronicznej bankNOWY24 należy dokonywać poprzez stronę Banku (http://www.banknowy24.pl)

iii. Przed zalogowaniem do bankNOWY24 należy zweryfikować czy w polu adresowym przeglądarki pierwszą częścią adresu są litery ”https” oraz czy sesja jest szyfrowana, a certyfikat został wydany dla witryny www.banknowy24.pl.

iv. Nie wolno logować się za pośrednictwem linków otrzymanych w wiadomościach e-mail lub SMS. Na stronie https://bezpiecznapoczta.cert.pl/ jest możliwość weryfikacji czy serwis poczty elektronicznej jest zabezpieczony zalecanymi technologiami.

v. W celu zapewnienia bezpieczeństwa korzystania z usług bankowości elektronicznej bankNOWY24, a także innych czynności wykonywanych w Internecie należy korzystać z legalnego i aktualnego oprogramowania antywirusowego, systemu operacyjnego oraz przeglądarek internetowych.

vi. Podczas korzystania z usług bankowości elektronicznej bankNOWY24 należy weryfikować poprawność wykonywanych operacji,

vii. Po wprowadzeniu danych do formularza przelewu elektronicznego, należy sprawdzić poprawność danych – w szczególności numer rachunku bankowego oraz kwotę przelewu.

viii. Należy każdorazowo weryfikować treść SMS-ów autoryzacyjnych, w szczególności sprawdzając numer rachunku odbiorcy przelewu, a także jego kwotę.

ix. Po zakończeniu korzystania z usług bankowości elektronicznej bankNOWY24, a także w przypadku oddalenia się od sprzętu, z którego następuje logowanie do bankowości elektronicznej bezwzględnie należy wylogować z serwisu.

x. Nie należy odpowiadać na wiadomości SMS i/lub e-mail, które pochodzą z nieznanych źródeł oraz nie należy korzystać z zamieszczonych w wiadomości

linków i załączników – mogą one zawierać wirusy, które mogą zostać pobrane na urządzenie.

xi. Nie należy instalować aplikacji spoza sklepu producenta (np. Google Play, App Store), a także oprogramowania umożliwiającego zdalny dostęp do urządzenia (np. AnyDesk, TeamViewer, QuickSupport).

xii. Nie należy logować się do bankowości internetowej w trakcie udostępniania osobie trzeciej swojego pulpitu.

xiii. Należy zachować szczególną ostrożność przy odbieraniu połączeń z nieznanych numerów telefonu. W przypadku odebrania i braku pewności, kim jest rozmówca – należy się rozłączyć. Jeżeli dzwoniący podawał się za Pracownika banku i informował, że na rachunku bankowym dzieje się coś złego – należy skontaktować się z infolinią Banku Nowego.

xiv. Przed zleceniem przelewu należy zweryfikować, kim jest jego odbiorca – należy poszukać informacji na temat danej osoby w Internecie i przeczytać opinie, komentarze na jej temat. Należy zachować ostrożność i zrezygnować z transakcji, jeżeli nie ma się pewności co do wiarygodności osoby dla której zleca się przelew środków.

xv. Nie należy podawać nieznajomym wrażliwych informacji na swój temat, a także nie należy udostępniać nigdzie oraz nikomu takich danych jak login i hasło do bankowości, PIN do bankowości lub kod autoryzujący SMS.

xvi. Zawsze należy uważnie czytać SMS-y z Banku oraz komunikaty autoryzacyjne. Nie należy akceptować operacji i transakcji, których się nie rozpoznaje

3. Karty płatnicze

1) Rodzaje Kart, jakie Bank oferuje dla danego typu Konta

Bank oferuje kartę Visa Debit dla rachunku oszczędnościowo – rozliczeniowego noweKONTO OSOBISTE.

2) Możliwość zapisania danych Karty w danym portfelu cyfrowym

Istnieje możliwość zapisania karty Visa Debit w portfelu cyfrowym Google Pay.

3) Zastrzeganie karty płatniczej

a. W jakiej sytuacji należy zastrzec kartę?

i. utraty karty płatniczej,

ii. otrzymania wiadomości SMS z kodem autoryzacyjnym (3D Secure) pomimo nie dokonywania żadnych operacji kartą,

iii. podejrzenia posiadania danych karty przez osoby trzecie (w tym np. uzyskaniu informacji o wycieku danych z serwisów internetowych),

b. Jak zastrzec kartę płatniczą?

i. W celu zastrzeżenia karty płatniczej należy skontaktować się telefonicznie z Centrum Komunikacji Santander Bank Polska S.A. na numer telefonu: +48 61 856 52 78;

ii. Zastrzeżenia w formie telefonicznej można dokonać 24 godziny na dobę przez 7 dni w tygodniu;

iii. Kartę płatniczą można również zastrzec w dowolnej placówce Banku Nowego S.A., w godzinach jej funkcjonowania.

4) Aktualne ostrzeżenie i rekomendacje Banku, w zakresie bezpieczeństwa korzystania z Karty oraz wykonywania za jej pośrednictwem Transakcji płatniczych, publikowane są na stronie internetowej Banku. Poniżej przedstawiono ostrzeżenia dotyczące najczęściej występujących oszustw oraz rekomendacji w zakresie bezpieczeństwa.

a. Ostrzeżenia w zakresie bezpieczeństwa

i. Ostrzeżenie przed zdalnym klonowaniem karty płatniczej – ostrzegamy przed oszustwem, w którym przestępcy podszywają się pod pracownika Banku i informują, że środki pieniężne na rachunku są zagrożone. W celu ich ochrony należy utworzyć rachunek techniczny, na który zostaną przelane pieniądze. Następnie przesyłają wiadomość SMS z linkiem do pobrania aplikacji, która rzekomo ma służyć do połączenia karty płatniczej z nowoutworzonym rachunkiem. W tym celu należy włączyć zainstalowaną aplikację i przyłożyć kartę do telefonu. W rzeczywistości aplikacja służy do „przedłużenia" sygnału NFC (służący np. do płatności zbliżeniowych) pomiędzy telefonami, dzięki czemu oszust stojący przy bankomacie może zbliżeniowo wypłacić środki z rachunku bankowego. Bankomat komunikuje się z kartą ofiary za pośrednictwem dwóch telefonów - najpierw złodzieja, a następnie ofiary, zatem karta ofiary musi cały czas pozostawać przyłożona do telefonu ofiary.

b. Rekomendacje Banku w zakresie bezpieczeństwa

i. Należy chronić dane swojej karty płatniczej – pamiętaj, że są to **dane poufne (!)** służące do autoryzacji transakcji. Podawaj je tylko jeśli chcesz zapłacić za towar lub usługę. Pamiętaj, że nie musisz podawać danych karty, jeśli to Ty masz być odbiorcą płatności.

ii. Należy kierować się zasadą ograniczonego zaufania! - nigdy nie masz pewności, kto znajduje się po "drugiej stronie", a bycie podejrzliwym to dla Ciebie najlepsza ochrona!

iii. Należy mieć ustawione jak najniższe limity dla płatności kartowych – niskie limity: dzienny oraz kwotowy pojedynczej operacji bezgotówkowej sprawiają, że po przekroczeniu ustalonej sumy, kolejne transakcje są blokowane. Dzięki temu, w przypadku utraty karty, osoba trzecia nie będzie mogła ukraść wszystkich środków z rachunku.

iv. Nie należy instalować aplikacji spoza sklepu producenta (np. Google Play, App Store), a także oprogramowania umożliwiającego zdalny dostęp do urządzenia (np. AnyDesk, TeamViewer, QuickSupport).

v. Nie należy odbierać połączeń z nieznanych numerów telefonu. W przypadku odebrania i braku pewności, kim jest rozmówca – należy się rozłączyć. Jeżeli dzwoniący podawał się za Pracownika banku i informował, że na rachunku bankowym dzieje się coś złego – należy skontaktować się z infolinią Banku Nowego.

vi. Nie należy odpowiadać na wiadomości SMS i/lub e-mail, które pochodzą z nieznanych źródeł oraz nie należy korzystać z zamieszczonych w wiadomości linków i załączników – mogą one zawierać wirusy, które mogą zostać pobrane na urządzenie. Na stronie https://bezpiecznapoczta.cert.pl/ jest możliwość weryfikacji czy serwis poczty elektronicznej jest zabezpieczony zalecanymi technologiami.

vii. Należy zwracać uwagę na niespodziewane wiadomości SMS dotyczące dodania karty do cyfrowego portfela Google (aplikacja Google Pay) - jeżeli sam nie próbujesz dodać karty do portfela, to nie potwierdzaj takich operacji oraz nie podawaj nikomu kodu autoryzującego. Nie należy wpisywać go też na żadnej stronie internetowej. Jeśli to zrobisz, oszuści będą mogli posługiwać się Twoją kartą za pośrednictwem Google Pay.

viii. Należy weryfikować subskrypcje, do których zapisywana jest karta - oszuści często tworzą strony, na których oferują darmowy (lub bardzo tani) okres próbny, aby następnie obciążać rachunek znacznie większymi kwotami. Przed zaakceptowaniem regulaminu i warunków korzystania z usługi, należy je przeczytać.

ix. Nie należy podawać nieznajomym wrażliwych informacji na swój temat, a także nie należy udostępniać nigdzie oraz nikomu takich danych jak numer karty płatniczej, data ważności karty, numer CVC/CVV, PIN do karty lub kod autoryzujący SMS.

x. Zawsze należy uważnie czytać SMS-y z Banku oraz komunikaty autoryzacyjne. Nie należy akceptować operacji i transakcji, których się nie rozpoznaje.

xi. Nie należy podawać swoich danych osobowych i/lub danych karty płatniczej na stronach, na które zostanie się przekierowanym po zeskanowaniu kodu QR lub kliknięciu w link albo w reklamę np. w mediach społecznościowych.

xii. Zawsze należy weryfikować adres strony, na której podaje się dane osobowe lub dane karty płatniczej – powinien co najmniej zaczynać się od "https://", a strona powinna być zabezpieczona certyfikatem SSL.

4. Bezpieczeństwo – informacje ogólne

1) Aktualne ostrzeżenia i rekomendacje Banku, w zakresie bezpieczeństwa korzystania z usług oferowanych przez Bank, publikowane są na stronie internetowej Banku. Poniżej przedstawiono ostrzeżenia dotyczące najczęściej występujących oszustw oraz rekomendacje w zakresie bezpieczeństwa.

a. Ostrzeżenia w zakresie bezpieczeństwa

i. **Ostrzeżenie przed PHISHING-iem**– uważaj na fałszywe wiadomości e-mail, w których oszuści podszywają się pod zaufane instytucje lub osoby, w tym za Bank Nowy. W treści wiadomości przestępcy nakłaniają do kliknięcia w złośliwe linki lub zeskanowania kodów QR, prowadzących zwykle do stron wyłudzających dane osobowe oraz poufne informacje, takie jak np. login i hasło do bankowości elektronicznej. Na stronie https://bezpiecznapoczta.cert.pl/ jest możliwość weryfikacji czy serwis poczty elektronicznej jest zabezpieczony zalecanymi technologiami.

ii. **Ostrzeżenie przed VISHING-iem** – ostrzegamy przed połączeniami telefonicznymi z nieznanych numerów lub z podstawionych numerów telefonów, które należą do zaufanych instytucji lub osób. Oszuści podczas

kontaktu podszywają się m.in. pod pracowników banków, w tym Pracowników Infolinii/Bezpieczeństwa Banku Nowego i pod presją czasu nakłaniają do określonych działań, np. podania danych logowania do bankowości elektronicznej lub otrzymanych kodów SMS, instalacji dodatkowej aplikacji, wykonania przelewu na rachunek bezpieczny/techniczny.

iii. **Ostrzeżenie przed SMISHING-iem** – uważaj na fałszywe wiadomości SMS, w których oszuści podszywają się pod zaufane instytucje lub osoby. W treści wiadomości przestępcy nakłaniają do kliknięcia w złośliwe linki lub o kontakt np. poprzez komunikat WhatsApp, pod pretekstem m.in. konieczności dopłaty do zamówionej paczki, rzekomej blokady rachunku bankowego lub podszywając się pod dziecko, któremu zepsuł się telefon. Linki prowadzą zwykle do stron wyłudzających dane osobowe oraz poufne informacje, takie jak np. login i hasło do bankowości elektronicznej.

iv. **Ostrzeżenie przed fałszywymi inwestycjami** – uważaj na reklamy i ogłoszenia publikowane przez oszustów w mediach społecznościowych, a także na wiadomości SMS czy e-mail, dotyczące inwestycji, na których można dużo zarobić. W przypadku podjęcia kontaktu z oszustami, ofiara początkowo proszona jest o przelanie niskiej kwoty na podany numer rachunku (najczęściej innej ofiary). Następnie przedstawiane jej są rzekome zyski z inwestycji. Ofiara może również otrzymywać na swój rachunek bankowy niewielkie kwoty (zyski) od oszustów, aby uśpić jej czujność. Z czasem ofiara jest nakłaniana do przelewania coraz wyższych kwot, a w momencie, w którym chce wycofać się z inwestycji – kontakt z oszustami po prostu się urywa.

v. **Ostrzeżenie przed oszustwami na legendę** – ostrzegamy przed oszustwem, które polega na podszywaniu się przestępcy pod inną osobę, np. członka rodziny, policjanta, pracownika banku itd. Jego celem jest wyłudzenie pieniędzy. Oszustwo to opiera się głównie na kontakcie telefonicznym – przestępca przedstawia się jako np. pracownik banku, podając fałszywe imię i nazwisko, a następnie informuje o zagrożeniu: np. o włamaniu na konto bankowe. Celem oszustów jest pozyskanie środków pieniężnych od ofiary lub danych logowania do bankowości elektronicznej. Przestępcy mogą również nakłaniać do pobrania specjalnych aplikacji, które rzekomo będą miały

chronić środki na koncie bankowym, a w rzeczywistości umożliwią oszustom zdalny dostęp do urządzenia ofiary.

vi. Ostrzeżenie przed oszustwem nigeryjskim – ostrzegamy przed procederem przestępczym, w którym oszuści początkują znajomość np. przez media społecznościowe, portale randkowe lub e-mail z przypadkową osobą. Poprzez kontakt na komunikatorach zdobywają zaufanie i sympatię, a następnie stosując manipulację wyłudzają od ofiary pieniądze lub dane logowania do bankowości elektronicznej. Oszustwo to jest podobne do oszustwa "na legendę", jednak w tym przypadku przestępcy bazują na długotrwałej znajomości i zdobytym zaufaniu, a nie na presji czasu i konieczności szybkiego działania.

b. Rekomendacje Banku w zakresie bezpieczeństwa

i. W celu posiadania bieżących informacji w zakresie cyberbezpieczeństwa zalecamy korzystanie z baz wiedzy znajdujących się w aplikacji mObywatel/ zakładka *Bezpiecznie w sieci* oraz na stronie https://cert.pl/.

2) Stosowane przez producentów oprogramowania sposoby oznaczania niezabezpieczonych lub niebezpiecznych stron internetowych; adresy stron internetowych, zidentyfikowane przez Bank jako niebezpieczne lub niezabezpieczone;

a. Wybrane przeglądarki tj. Google Chrome, Microsoft Edge, Mozilla Firefox oznaczają strony, które nie posiadają certyfikatu SSL jako niezabezpieczone lub niebezpieczne. Przed wyświetleniem takiej strony pojawia się informacja, iż połącznie nie jest bezpieczne/ połączenie nie jest prywatne oraz „Osoby atakujące mogą wykraść dane z tej witryny". Prezentowane są dwa łącza: jedno umożliwia przejście dalej na stronę; drugie cofa do poprzedniej strony.

b. Na podstawie art. 20 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej CSIRT NASK prowadzi Listę Ostrzeżeń domen internetowych, które mogą wprowadzić w błąd użytkownika lub służą do realizacji oszukańczych celów cyberprzestępców. Lista Ostrzeżeń znajduje się na stronie: https://cert.pl/ .