BEZPIECZEŃSTWO USŁUG PŁATNICZYCH

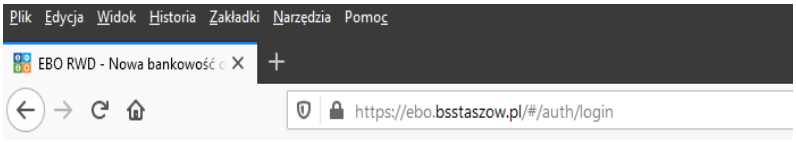
11 zasad cyberbezpieczeństwa

1. **Nie otwieraj załączników** z niepewnych źródeł i nie klikaj w podejrzane linki.
2. **Sprawdzaj adresy stron www**, na których się logujesz, a także ich **certyfikaty**.
3. **Regularnie aktualizuj** oprogramowanie na urządzeniach, na komputerze i telefonie (system, aplikacje, przeglądarkę, antywirusy).
4. **Twórz skomplikowane hasła** trudne do odgadnięcia przez postronne osoby.
5. **Nie używaj tego samego hasła** do różnych kont oraz **nie zapisuj haseł** na kartkach ani w jawnych plikach (niezaszyfrowanych) na komputerze.
6. **Nie podawaj / nie wysyłaj** swoich loginów i haseł innym osobom.
7. **Nie loguj się przez publiczne, niezabezpieczone wi-fi** do serwisu internetowego eBO i aplikacji eBO mobile.
8. **Nie loguj się do bankowości elektronicznej na urządzeniach publicznie dostępnych** np. w kafejkach, hotelach.
9. **Czytaj treść SMS** przed potwierdzeniem transakcji.
10. **Nie podłączaj zewnętrznych nośników danych** do swojego urządzenia, jeśli nie masz pewności co do ich bezpieczeństwa.
11. Zainstaluj i aktualizuj oprogramowanie antywirusowe.

Chroń komputer i telefon

- Loguj się do bankowości elektronicznej na urządzeniach z legalnym oprogramowaniem i aktualną przeglądarką
- Pobieraj aplikację mobilną eBO mobile i jej aktualizacje z autoryzowanych sklepów: Google Play, App Store, App galery
- Blokuj dostęp do telefonu i komputera
- Używaj zapory sieciowej (firewall) i systematycznie skanuj komputer programem antywirusowym
- Nie lekceważ komunikatów bezpieczeństwa – w tym komunikatów banku
- Nie instaluj na komputerze oprogramowania z nieznanych źródeł – nigdy nie przesyłamy linków i załączników do dodatkowych zabezpieczeń w postaci np. certyfikatu e-security, aplikacji antywirusowej lub innego dodatkowego oprogramowania
- Nie otwieraj wiadomości o podejrzanych treściach ani ich załączników. Zachowuj ostrożność i ograniczone zaufanie do maili i SMSów, w których:
  - widzisz prośbę o zalogowanie do serwisu internetowego banku przez specjalnie umieszczony link
  - ktoś prosi Cię o dane do logowania, login, hasło, kod z narzędzia autoryzacji
- Sprawdź szczegółowe informacje na temat bezpiecznego korzystania z aplikacji eBO mobile

Na co uważać przy logowaniu do konta w przeglądarce?



- **Upewnij się, czy logujesz się na poprawnej stronie z certyfikatem bezpieczeństwa** (zamkniętą kłódką). Adres https://ebo.bsstaszow.pl najlepiej wpisać ręcznie.
- **Sprawdź, czy strona logowania wyświetla się poprawnie** i pokazują się na niej wszystkie elementy. W razie wątpliwości przerwij logowanie i skontaktuj się z bankiem.
- **Sprawdzaj datę i godzinę ostatniego (nie-)poprawnego logowania**

Pamiętaj o 2 ważnych zasadach bezpieczeństwa

Ostrzegamy przed wiadomościami, które nakłaniają do zainstalowania aplikacji na Twoim urządzeniu. Przypominamy też, że podczas logowania do aplikacji eBO mobile nigdy nie poprosimy Cię o dane logowania do bankowości elektronicznej eBO.

- Uważaj na wszelkie wiadomości, np. SMS lub powiadomienia push z nieznanych źródeł, w których dostajesz prośbę o kliknięcie w link i zainstalowanie aplikacji na swoim urządzeniu. W rzeczywistości oszuści chcą zdobyć Twoje narzędzie autoryzacji lub poufne dane do logowania
- Do logowania do aplikacji eBO mobile podawaj tylko PIN lub loguj się odciskiem palca.

Jeżeli widzisz w aplikacji eBO mobile prośbę o podanie danych logowania do bankowości elektronicznej eBO, może to oznaczać, że masz na telefonie złośliwe oprogramowanie i doszło do próby wyłudzenia od Ciebie poufnych danych

Pamiętaj!

- Nie wyrażaj zgody na zainstalowanie na urządzeniu aplikacji pochodzących z **nieznanych źródeł**
- Nie wyłączaj producenckich mechanizmów bezpieczeństwa na Twoim urządzeniu
- Nie wykonuj działań, o które prosi nieznany Ci nadawca w SMS-ie/wiadomości email (np. klikanie w linki)

Uważaj na telefoniczne próby podszywania się pod pracowników banku

Ostrzegamy przed telefonami od nieznanych Ci osób, które podają się za pracowników banku, powołują się na względy bezpieczeństwa i nakłaniają do zainstalowania aplikacji na Twoim urządzeniu.

O co mogą prosić Cię osoby, które podszywają się pod pracowników banku?

- o podanie poufnych danych
- o pobranie ze sklepu Google Play i **zainstalowanie na telefonie, tablecie lub komputerze aplikacji do zdalnej weryfikacji**, np. TeamViewer QuickSupport.

W rzeczywistości oszuści chcą zdobyć Twoje:

- dane do logowania do bankowości elektronicznej
- narzędzie autoryzacyjne

Tak wyłudzone dane można użyć do wykonania przelewu z Twojego konta na nieznany Ci rachunek.

1. **Pracownik banku podczas rozmowy telefonicznej nigdy nie poprosi Cię o podanie mu haseł dostępu** do żadnego z serwisów (internetowego, mobilnego, telefonicznego).

W sytuacji, gdy odbierzesz telefon od osoby podającej się za pracownika banku, masz jakiekolwiek wątpliwości, czy zasadne jest podawanie kodu z narzędzia autoryzacyjnego lub innych danych, jak również w każdym innym przypadku, w którym podczas korzystania z elektronicznych kanałów dostępu spotkasz się z sytuacją, która wyda Ci się nietypowa, podejrzana lub wzbudzi Twoje zaniepokojenie, skontaktuj się z nami.

<u>Uważaj na fałszywe SMSy z linkami do wykonania przelewu</u>

Fałszywe SMS-y zawierają linki do realizacji przelewu i przenoszą do stron, które podszywają się pod stronę banku.

Podanie na fałszywej stronie poufnych danych do bankowości elektronicznej i kodu z narzędzia autoryzacji skutkuje ich przejęciem przez przestępców

Pod kogo mogą się najczęściej podszywać nadawcy fałszywych SMS-ów?

- znane portale ogłoszeniowe, sprzedażowe i aukcyjne
- firmy kurierskie i telekomunikacyjne
- instytucje państwowe, urzędy, itp.

Jaka może być treść fałszywych SMS-ów?

- informacja o konieczności odblokowania konta na danym portalu
- informacja o możliwości zapobieżenia przekazaniu pieniędzy do rezerw NBP w związku ze specustawą dotyczącą koronawirusa
- prośba o dopłacenie niewielkiej kwoty za przesyłkę
- informacja o konieczności spłaty zadłużenia, np. za zaległą fakturę
- informacja o konieczności dopłaty do podatku
- informacja o konieczności zapłaty za przedłużenie aukcji/ogłoszenia

Niebezpieczeństwo przechwycenia Twoich danych (danych do logowania i kodu z narzędzia autoryzacji) – z czym się wiąże?

Oszust może zyskać możliwość logowania się do Twojej bankowości elektronicznej i zlecania operacji, np.: utworzenia szablonu płatności lub wykonania przelewu na wskazany przez siebie numer rachunku odbiorcy.

Przypominamy!

1. Zachowaj ostrożność i ograniczone zaufanie do wiadomości od nieznanych nadawców, w których znajduje się prośba o skorzystanie z linku – nie reaguj na nie, **nie klikaj w linki**, **nie ujawniaj swoich danych**.
2. Logując się do serwisu internetowego banku, zawsze wprowadzaj adres strony ręcznie – **nie korzystaj z linków!**
3. **Sprawdzaj poprawność** adresu strony w przeglądarce internetowej (poprawny adres zaczyna się od https://ebo.bsstaszow.pl
4. **Przed potwierdzeniem operacji zlecanej w eBO kodem SMS przeczytaj dokładnie treść otrzymanego SMS-a, żeby upewnić się, że dotyczy on właściwej operacji** (zwróć uwagę na **rodzaj dyspozycji**, poprawność numeru konta odbiorcy, **kwotę przelewu**).

<u>Uwaga na fałszywe wiadomości SMS, Messenger, Facebook</u>

Ostrzegamy przed fałszywymi wiadomościami:

- **SMS, zawierającymi linki do dokonania płatności,**
- **w serwisie Facebook i aplikacji Messenger, w których oszuści podszywają się pod Twoich znajomych i proszą o przelew BLIK lub o przekazanie kodu BLIK.**

Zachowaj ostrożność!

- Jeśli otrzymasz wiadomość SMS z prośbą o dopłacenie niewielkiej kwoty za dostarczenie przesyłki, odblokowanie konta na danym portalu, przedłużenie okresu wystawienia ogłoszenia, itp., bądź dotyczącą usługi SMS Premium, zawierającą link do dokonania płatności – nie korzystaj z linku: nadawca może podszywać się pod firmę kurierską bądź powszechnie znane portale ogłoszeniowe, sprzedażowe, aukcyjne i inne. W rzeczywistości link umieszczony w SMSie prowadzi do fałszywej strony pośrednika płatności, a następnie – na fałszywą stronę banku, i ma na celu wyłudzenie poufnych danych do bankowości elektronicznej oraz kodu z narzędzia autoryzacyjnego.
- Jeśli otrzymasz od znajomego prośbę o przelew BLIK **lub o przekazanie kodu BLIK** - zadzwoń do tej osoby i potwierdź jej prośbę.

Przypominamy!

1. Zachowaj ostrożność i ograniczone zaufanie w stosunku do wiadomości od nieznanych nadawców, w których znajduje się **prośba o przelew** lub **skorzystanie z linku** – nie reaguj na nie i **nie ujawniaj swoich danych**.
2. Logując się do serwisu internetowego Banku, zawsze wprowadzaj adres strony ręcznie – **nie korzystaj z linków!**
3. **Sprawdzaj poprawność adresu strony**, widniejącego w przeglądarce internetowej (poprawny adres zaczyna się od : http://www.bsstaszow.pl
4. **Przed potwierdzeniem operacji zlecanej w serwisie eBO kodem SMS przeczytaj uważnie treść otrzymanego SMS-a, aby upewnić się, że dotyczy on właściwej operacji** (zwróć uwagę na rodzaj dyspozycji, poprawność numeru rachunku odbiorcy, kwotę transakcji).

5. Korzystaj z dwuskładnikowego uwierzytelnienia logowania do kont na Facebooku i innych serwisach społecznościowych. Nie podawaj nikomu danych do logowania do serwisu internetowego i serwisów społecznościowych, aby uniknąć przejęcia tych danych przez niepowołane osoby.

Wirtualne waluty – na co uważać?

Wirtualna waluta (tzw: kryptowaluta) to nie pieniądz. Zanim zdecydujesz się zainwestować swoje oszczędności w wirtualne waluty, sprawdź ryzyka.

- **Ryzyko kradzieży Twoich pieniędzy** - np. z powodu cyberataku na podmiot, który prowadzi wymianę walut wirtualnych
- **Ryzyko braku gwarancji Bankowego Funduszu Gwarancyjnego**
- **Ryzyko braku powszechnej akceptowalności**. Punkty usługowo-handlowe nie mają obowiązku akceptowania walut wirtualnych.
- **Ryzyko oszustwa.** Niektóre oferowane formy inwestowania w waluty wirtualne mogą mieć charakter piramidy finansowej. W przypadku takiego oszustwa, jedyną formą ochrony będzie postępowanie karne. Pamiętaj, że żadne polskie instytucje ochrony inwestorów czy konsumentów (Urząd Ochrony Konkurencji i Konsumentów, Komisja Nadzoru Finansowego) nie mają prawnych możliwości pomocy.
- **Ryzyko dużej zmiany ceny**. Do tej pory ceny wirtualnych walut charakteryzowały się wysoką zmiennością.

Jakich metod używają oszuści?

- Podszywają się pod pośredników lub brokerów inwestycyjnych
- Powołują się na sfałszowane wypowiedzi znanych osób, np. sportowców, aktorów, dziennikarzy
- Zachęcają do rejestracji w programie inwestycyjnym i obiecują nieprzeciętne zyski, np. dzięki „dźwigni finansowej”
- Proszą o:
    - zrobienie przelewu rejestracyjnego
    - zrobienie przelewu przez eBO, eBO mobile, telefon, SMS, komunikator internetowy lub przelewu w Twoim imieniu
    - podanie danych do logowania i autoryzacji (np. kody SMS), kodów BLIK
    - zainstalowania dodatkowego oprogramowania
- Proszą o zrobienie zdjęcia dowodu osobistego lub karty płatniczej

W rzeczywistości oszuści chcą zdobyć Twoje dane i wykorzystać je do kradzieży pieniędzy z konta.

Możesz podejrzewać, że Ty lub bliska osoba możecie być ofiarami oszustwa, gdy

- Firma pośrednicząca w inwestycjach nie jest zarejestrowana w UE (aby prowadzić działalność brokerską w Polsce, konieczne jest posiadanie licencji jednego z krajów UE)
- Ktoś, kogo nie znasz, zrobił Ci przelew i prosi o przesłanie go komuś innemu
- Masz jakiekolwiek obawy, co do legalności inwestycji oraz podmiotu, który w nich pośredniczy

Vhishing, czyli voice phishing

Przestępcy telefonicznie podszywają się pod firmy usługowe, informatyczne, lub policję. Pretekst do podania poufnych danych może być różny, np. awaria systemów, prowadzone przez policję śledztwo czy zagrożenie utraty pieniędzy.

Oszuści często podają się za pracowników banku i proszą w trakcie rozmowy o podanie loginu i hasła do bankowości internetowej, a potem kodu SMS. Następnie wykorzystują te informacje do zmiany numeru telefonu, którego używasz do autoryzacji transakcji. Wyłudzony kod może posłużyć także do zlecenia innych dyspozycji.

Smishing

Przestępcy wysyłają SMS-y, które często dotyczą konta bankowego, np. piszą o konieczności anulowania niezlecanego przez Ciebie przelewu (odmiana phisingu).

W wiadomościach namawiają do kontaktu pod wskazany numer telefonu lub do wejścia w link. Połączenie najczęściej odbiera automatyczny serwis telefoniczny, który prosi o podanie poufnych danych, np.: osobowych, do logowania, danych karty płatniczej czy z narzędzia autoryzacji transakcji.