Przewodnik dla Klienta w zakresie bezpiecznego korzystania z bankowości elektronicznej

1. Uważaj na fałszywe wiadomości e-mail

Bank Spółdzielczy w Jarocinie nigdy nie wysyła do swoich klientów wiadomości mailowych z prośbami o podanie poufnych informacji (uzupełnienie formularzy). Nie należy zatem odpowiadać na takie wiadomości i nie uruchamiać zawartych w nich linków. Złodzieje często podszywają się pod bankowców i fałszują korespondencję, a nawet witryny internetowe, które do złudzenia przypominają oryginalne z Banku. Wiadomości e-mail wysyłają do tysięcy osób w nadziei na złapanie naiwnego Klienta, który dobrowolnie poda wrażliwe dane takie jak hasło i login do serwisu bankowości internetowej. Działania takie określa się terminem „phishing", który pochodzi od słowa „fishing" – łowienie. Dlatego każdą tego typu informację należy bezwzględnie zignorować i **pod żadnym pozorem**

nie korzystać z linków przesłanych w wiadomości e-mail. Takie działanie jest przestępstwem internetowym. W takiej sytuacji najlepiej **poinformować** o tym Bank. Zalecamy jednak **unikać** odbierania **poczty elektronicznej** na stacji roboczej, na której korzystamy z usług bankowości elektronicznej. To pozwoli ograniczyć ryzyko zainfekowania naszego urządzenia złośliwym oprogramowaniem, które potencjalnie może pochodzić z zainfekowanej wiadomości e-mail. Należy zwrócić **szczególną uwagę** na załączniki, które mogą zawierać złośliwe oprogramowanie lub skrypty umożliwiające pobranie ich z sieci Internet. Załączniki powinny być przeskanowane **przed otwarciem** przez oprogramowanie **antywirusowe** zainstalowane na stacji roboczej lub urządzeniu mobilnym. Zalecamy korzystanie z usług serwerów poczty e-mail wyposażonych w system antyspamowy oraz antywirusowy dla kont pocztowych. System taki może spowodować, że wybrane wiadomości e-mail zostaną oznaczone jako stwarzające potencjalne zagrożenie i w efekcie mogą zostać odrzucone.

2. Sprawdź adres strony logowania do CUI lub eBO

Do logowania do systemu należy używać wyłącznie adresu podanego przez Bank wpisując go do paska adresu przeglądarki internetowej lub skorzystać **bezpośrednio** ze strony naszego Banku. W Banku Spółdzielczym w Jarocinie funkcjonują trzy adresy. Dla klientów korzystających z bankowości internetowej CUI logujących się za pomocą tokena lub hasła maskowanego wybieramy adres: https://ebank2.cui.pl/jarocin, dla klientów korzystających z usługi korporacyjnej CUI wybieramy adres:

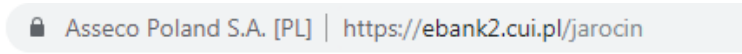
https://ebank2.cui.pl/jarocin_k, natomiast dla Klientów korzystających z bankowości internetowej eBO wybieramy adres: https://ebo.bsjarocin.pl. Do wyszukiwania adresów nie powinno używać się wyszukiwarki internetowej. Dla poprawy bezpieczeństwa nie należy umieszczać strony logowania wśród „ulubionych" stron przeglądarki internetowej. Przestępcy tworzą bowiem oprogramowanie, które jest w stanie wykorzystać luki w systemie i podmienić stronę na fałszywą. O tym, że znajdujemy się na właściwej stronie internetowej, informuje nas pasek adresu. Adres musi zaczynać się od https:// a przeglądarka powinna zweryfikować połączenie wyświetlając symbol zamkniętej kłódki. **Bardzo ważne** jest i należy **zawsze** sprawdzić, czy adres strony jest **właściwy** i nie zawiera tzw. „literówek". Poprawne adresy wyglądają następująco:

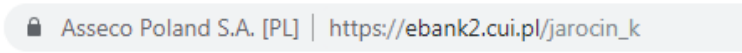
- W bankowości CUI:

Dla przeglądarki Internet Explorer:

Dla przeglądarki Firefox:

Dla przeglądarki Chrome:





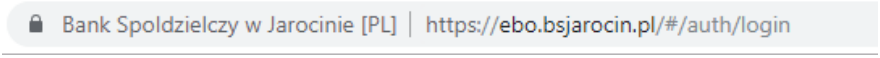
Wybierając ***"Wyświetl certyfikaty"*** lub ***"Więcej informacji"*** możemy zweryfikować czy certyfikat strony wystawiony jest dla Centrum Usług Internetowych przez firmę **DigiCert Inc.** Certyfikat wystawiony jest dla CUI, którego właścicielem jest firma **Asseco Poland S.A.** Brak "zatrzaśniętej kłódki" oznacza, że mamy do czynienia z niebezpiecznym połączeniem, w którym dane nie są szyfrowane - w związku z tym nie powinniśmy podejmować prób logowania na taką stronę.

- W bankowości eBO:

Dla przeglądarki Internet Explorer:

Dla przeglądarki Firefox:

Dla przeglądarki Chrome:



Wybierając ***"Wyświetl certyfikaty"*** lub ***"Więcej informacji"*** możemy zweryfikować czy certyfikat strony wystawiony jest dla Właściciela: **Bank Spoldzielczy w Jarocinie** przez firmę **DigiCert Inc.** Brak symbolu bezpieczeństwa - "zatrzaśnięta kłódka" oznacza, że mamy do czynienia z niebezpiecznym połączeniem, w którym dane nie są szyfrowane - w związku z tym nie powinniśmy podejmować prób logowania na taką stronę.

3. Stosuj się do procedur Banku

Logując się na stronę Banku należy stosować się do procedur obowiązujących w Banku. Zasady bezpiecznego korzystania z bankowości elektronicznej zawarte są w niniejszym przewodniku, który jest także zamieszczony na stronie internetowej Banku: https://bsjarocin.pl

4. Aktualizuj przeglądarkę internetową i system operacyjny

Przeglądarka internetowa to program, który służy do otwierania stron internetowych, także tych do logowania do systemu bankowości internetowej. Należy zatem zadbać o to, by na naszym komputerze regularnie dokonywać aktualizacji oprogramowania. Zaleca się również używać firewalla. Hakerzy wyszukują luk w programach, za pomocą których mogą wykraść niezbędne informacje. Należy także pamiętać o **regularnej aktualizacji** sytemu operacyjnego. Dostawcy oprogramowania na bieżąco monitorują poziom bezpieczeństwa i publikują aktualizacje uzupełniające luki w oprogramowaniu. Nowoczesna przeglądarka

internetowa jest **niezbędnym** elementem zapewniającym bezpieczne korzystanie z systemu bankowości internetowej. Nie zastąpi jednak ludzkiej **czujności**, dlatego **nie instaluj** oprogramowania z **nieznanych** źródeł. Takie aplikacje mogą zawierać oprogramowanie szpiegujące, szyfrujące, czy złośliwe. **PAMIĘTAJ! Urządzenie mobilne** takie jak smartfon, tablet, itp. również posiada zainstalowany system operacyjny i podlega tym samym zasadom, co komputer lub laptop.

PAMIĘTAJ! dbając o bezpieczeństwo na swoim komputerze możesz nie tylko bezpiecznie korzystać z bankowości internetowej, ale również chronisz dane na nim przechowywane.

5. Korzystaj z oprogramowania antywirusowego

Równie niezbędne jak bezpieczna przeglądarka internetowa jest zainstalowanie programu antywirusowego zapobiegającego instalacji wirusów oraz innego szkodliwego oprogramowania. Zalecamy, aby **nie korzystać** z **darmowych** programów antywirusowych. Oprogramowanie zainstalowane na komputerze czy też urządzeniu mobilnym **powinno** posiadać **płatną licencję**. Warto przy tym korzystać z programów polecanych przez **ekspertów**, ponieważ nie wszystkie aplikacje dostępne w sieci spełniają niezbędne standardy. Należy pamiętać, że instalowanie aplikacji pobranych z niesprawdzonych stron internetowych bardzo często kończy się zainfekowaniem komputera przez oprogramowanie

szpiegujące. Warto także raz na kilka dni **skanować** antywirusem komputer i dbać o **aktualne** bazy wirusów.

6. Loguj się na własnym komputerze lub własnym urządzeniu mobilnym

Zaletą bankowości internetowej jest to, że dostęp do własnego konta możemy mieć z dowolnego komputera podpiętego do sieci. Tu jednak zaleca się duża ostrożność – powinniśmy korzystać przede wszystkim z naszego własnego stanowiska komputerowego lub naszego własnego urządzenia mobilnego. Nie powinniśmy także logować się na ogólnie dostępnych komputerach, np. w kafejkach internetowych, miejscach hotelowych, kioskach internetowych, itd. Nie mamy bowiem gwarancji, że komputery te są „czyste". Mogą tam być zainstalowane programy szpiegujące, które potrafią przechwycić dane do logowania czy numery kart. Jeśli jednak musimy skorzystać z obcego komputera należy pamiętać, by zawsze wylogować się z serwisu transakcyjnego. **Nie należy** dokonywać płatności i logować się do serwisów bankowości elektronicznej podając swoje hasło w punktach bezpłatnego publicznego dostępu do Internetu - w tzw. **hot-spotach**, np. na lotniskach, dworcach kolejowych, stacjach paliw, hotelach, itd. Takie sieci charakteryzują się często niskim poziomem bezpieczeństwa co jest dodatkowym czynnikiem stwarzającym **zagrożenie**.

7. Chroń środki dostępu do usługi internetowej

Nie zapisuj danych do logowania (identyfikatorów, haseł, itd.) - zarówno w formie tradycyjnej, elektronicznej jak również bezpośrednio w przeglądarce internetowej, gdyż w ten sposób stwarzasz zagrożenie przejęcia ich przez osoby postronne. Bez znaczenia jest tutaj forma - taka informacja zawsze może zostać przejęta przez niepowołaną osobę, dla przykładu, jeśli jest to urządzenie przenośne, takie jak notebook, tablet, czy telefon komórkowy, może zostać skradzione.

Staraj się także **okresowo zmieniać** hasło dostępu do konta. Bankowość eBO w każdym miesiącu na stronie logowania sugeruje Klientowi zmianę istniejącego hasła. **Zalecamy korzystać** z tej funkcjonalności. Także po zalogowaniu na stronie bankowości elektronicznej – w ustawieniach profilu Klienta udostępniona jest opcja zmiany hasła, której można dokonać w dowolnym momencie. Token lub karty chipowe do zatwierdzania transakcji internetowych trzymaj w bezpiecznym miejscu – nie zostawiaj na przykład w biurku w pracy. Pamiętaj, że są to dane, które mogą posłużyć do zlecenia przelewu z Twojego konta. Sprawdzaj także daty i godziny ostatniego logowania na rachunek, które znajdują się w zakładce Historia logowań.

PEŁNOMOCNICTWO DO RACHUNKU

Pamiętaj, aby **nigdy nie udostępniać** środków dostępu do rachunku innym osobom – **niezależnie** od tego, czy jest to osoba Tobie dobrze znana – **nie ma znaczenia**, czy jest to Współmałżonek, Córka, Syn czy Rodzic. **Twoje** środki autoryzacji są przeznaczone **TYLKO** do **Twojego** użytku. Udostępnianie danych logowania jest **niedopuszczalne**. Jeżeli istnieje potrzeba, aby także ktoś inny miał dostęp do Twojego rachunku, należy udać się do placówki Banku i podpisać dokument stanowiący ustalenie **pełnomocnictwa** do Twojego rachunku. **Pełnomocnik** otrzyma swoje **własne** środki dostępu do Twojego rachunku i **tylko** w ten sposób będzie uprawniony do korzystania z niego.

OBRAZEK BEZPIECZEŃSTWA

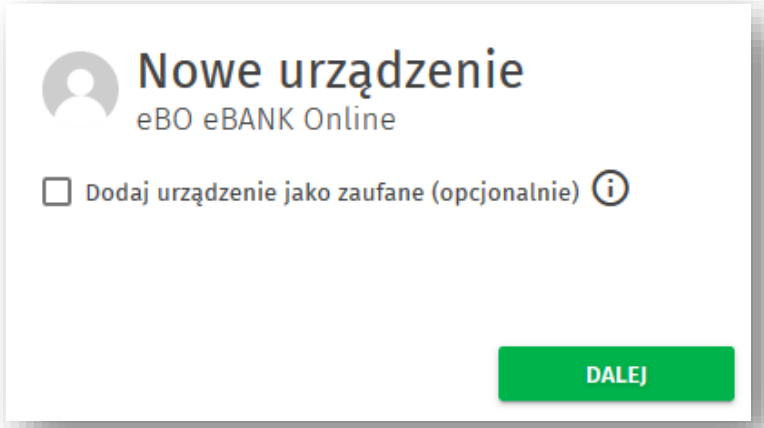
Bankowość internetowa eBO umożliwia dodanie **obrazka bezpieczeństwa**, który stanowi dodatkowy element zabezpieczeń. Zalecamy skorzystanie z tej możliwości. Obrazek można dostosować po zalogowaniu się do bankowości – w personalizacji profilu Klienta. **Zapamiętaj** ustawiony przez siebie obrazek - będzie on wyświetlany **każdorazowo** na stronie logowania po wpisaniu loginu. Zmiana wybranego obrazka jest dozwolona w dowolnym momencie po zalogowaniu się do bankowości – w ustawieniach profilu Klienta. Obrazek bezpieczeństwa poświadcza, że logujesz się do właściwej strony Banku Spółdzielczego w Jarocinie. Jeśli obrazek byłby inny niż wybrany przez Ciebie lub też nie byłby wyświetlony, **nie powinieneś** podejmować prób logowania.

LOGOWANIE DWUETAPOWE

Dodatkowym mechanizmem, który podnosi poziom bezpieczeństwa w bankowości eBO jest logowanie dwuetapowe. To rozwiązanie wymaga **dwuskładnikowego uwierzytelnienia**, którym jest hasło ustawione przez Klienta oraz ciąg znaków wygenerowany przez token lub kod SMS.

ZAUFANE URZĄDZENIE

Jest to mechanizm, który pozwala zdefiniować urządzenie, na którym system nie będzie wymagał drugiego składnika uwierzytelnienia, jakim jest ciąg znaków wygenerowany przez token lub kod SMS podczas logowania do bankowości. Procedura dodania urządzenia zaufanego odbywa się **podczas logowania**. System rejestruje urządzenie na liście urządzeń zaufanych, którymi można zarządzać w ustawieniach zabezpieczeń w menu **ZAUFANE URZĄDZENIA.** Logowanie z innego komputera – nie dodanego do listy urządzeń zaufanych wymaga mechanizmu dwuskładnikowego uwierzytelnienia. Warto pamiętać, iż system rozpoznaje także wersję przeglądarki internetowej, z której dodano urządzenie zaufane i przy próbie logowania z innej przeglądarki ponownie wymaga dwuskładnikowego uwierzytelnienia.



8. Ustaw silne hasło

Poprzez silne hasło rozumiemy ciąg znaków o odpowiednim stopniu złożoności. W bankowości internetowej CUI mamy możliwość nadania ciągu hasła o długości od 4-8 znaków. W bankowości internetowej eBO mamy możliwość nadania hasła składającego się z 8- 20 znaków. Skorzystaj z tych możliwości i nadaj hasło o maksymalnej długości. Ponadto staraj się, żeby hasło zawierało małe i duże litery oraz znaki specjalne. Im hasło jest bardziej skomplikowane i trudniejsze do zapamiętania dla potencjalnego przestępcy, tym bardziej możemy czuć się bezpieczni. **Unikaj** stosowania nazw własnych, takich jak imiona, nazwiska, nazwy miejscowości, daty urodzenia, nazwy firmy itp. - jest to zawsze dodatkowe ułatwienie przy próbie złamania dostępu. **Stosuj unikalne** hasła, tzn. inne dla każdego z serwisów, z których korzystasz.

Trzykrotne błędne wpisanie hasła powoduje blokadę dostępu do bankowości.

HASŁO MASKOWANE

Hasło maskowane to bezpieczny sposób wprowadzania hasła, polegający na wpisaniu do systemu jedynie losowo wyznaczonych znaków. Jest to dodatkowe zabezpieczenie przed udostępnieniem go osobom niepowołanym. **Pamiętaj**, że po błędnej próbie logowania system **nie zmienia** sekwencji wymaganych znaków hasła – prosi o podanie **tych samych** znaków hasła, których wymagał poprzednim razem. Gdyby system żądał wpisania innych znaków niż przy błędnej próbie, nie kontynuuj próby logowania i skontaktuj się z Bankiem, np.:

Pierwsza próba logowania:

Druga próba logowania:

1 + 2 sekwencja wpisania hasła = przestępca przejmuje całe hasło do bankowości

Podobnie, gdyby system wymagał wpisania wszystkich znaków w poszczególne pola hasła maskowanego, również nie podejmuj logowania i skontaktuj się z Bankiem.

9. Zwiększ kontrolę nad swoim kontem

USŁUGA IVR dla eBO

Bankowość eBO dysponuje **usługą IVR**, która pozwala na **samodzielne telefoniczne** zablokowanie dostępu do rachunku, w przypadku, gdy mamy podejrzenie, iż ktoś niepowołany może wejść w posiadanie naszych danych dostępowych i w efekcie uzyskać nieautoryzowany dostęp do naszego konta. Usługa ta umożliwia także **samodzielne odblokowanie** dostępu do rachunku w sytuacji, gdy podjęte przez Ciebie błędne próby logowania spowodowały zablokowanie identyfikatora. Usługa jest dostępna **24h/na dobę, przez 7 dni w tygodniu.** Z uwagi na jej całodobowe działanie pracownicy Banku nie dokonują odblokowania dostępu do rachunku na podstawie telefonicznych zgłoszeń – **Konieczna** jest wtedy **wizyta** Klienta w Banku.

Jak aktywować usługę IVR?

Usługa IVR jest dostępna po zalogowaniu w ustawieniach środków dostępu w zakładce **OBSŁUGA PRZEZ TELEFON**. Należy zaznaczyć opcję aktywacji oraz ustalić swój unikatowy numer PIN, aby usługa została poprawnie uruchomiona. Numer PIN możemy zmienić w dowolnym momencie w wyżej wymienionej zakładce. Aby skorzystać z usługi, **zadzwoń** na infolinię Banku: **62 747 00 00,** a następnie wybierz odpowiednio: *Obsługa bankowości elektronicznej lub kart płatniczych* wciskając **2** na swoim urządzeniu oraz w kolejnym kroku: *Nowa bankowość elektroniczna eBO*, wybierając **3**

i postępuj według odpowiednich wskazań automatycznej sekretarki.

Dla bankowości CUI

W bankowości CUI mamy możliwość zgłoszenia zastrzeżenia dostępu do rachunku poprzez infolinię Banku. **Zadzwoń** pod nr **62 747 00 00** – a następnie wybierz odpowiednio *Obsługa bankowości elektronicznej lub kart płatniczych* wciskając **2** na swoim urządzeniu oraz w kolejnym kroku: *Stara bankowość elektroniczna CUI,* ponownie wybierając **2**. Tym sposobem zostaniesz przekierowany do pracownika Banku.

POWIADOMIENIA SMS

Bardzo ważną kwestię dotyczącą bezpieczeństwa w środowisku bankowości elektronicznej stanowi także usługa **powiadomień o logowaniu**, która poinformuje Cię za pomocą wiadomości SMS o logowaniu do systemu bankowości elektronicznej. System bankowości eBO poinformuje Cię o **każdej udanej**, a także **nieudanej** próbie logowania. Bankowość eBO pozwala także na włączenie funkcjonalności powiadomień SMS o zmianie salda na rachunku, od wybranej przez Ciebie kwoty oraz stanu salda o określonej porze.

FILTRY LOGOWANIA

System bankowości elektronicznej CUI oraz eBO umożliwia dodatkowo skonfigurowanie **filtrów logowania**, które dopuszczą logowanie do Twojego konta **tylko** z określonych przez Ciebie adresów IP. Ponadto

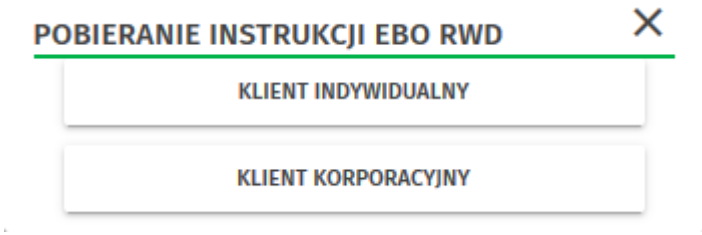
bankowość eBO daje możliwość wyboru wyznaczonych dni oraz przedziałów czasowych dostępności kanałów elektronicznych. Mechanizm ten jest dostępny w ustawieniach zabezpieczeń. Dla bankowości CUI klient musi złożyć wniosek w Banku lub poprzez bankowość, który zostanie następnie rozpatrzony.

LIMITY

Dodatkowym zabezpieczeniem, które możesz wprowadzić jest **limit** jednorazowy, dzienny oraz miesięczny, który uniemożliwia zlecenie transakcji przewyższających wyznaczoną całkowitą sumę. Limitami można zarządzać w ustawieniach limitów.

INFORMACJA DLA KLIENTA

Wszelkie informacje dotyczące bankowości eBO znajdziesz na stronie internetowej: https://ebo24.pl. Jest to **oficjalna strona** informacyjna dla Klientów. Instrukcje korzystania z bankowości elektronicznej eBO znajdują się na stronie logowania – możesz je pobrać klikając **znak,** (?) który znajduje się w prawym górnym rogu strony. Pojawi się menu wyboru instrukcji dla Klienta indywidualnego lub Klienta korporacyjnego.



10. Dbaj o dane swojej karty płatniczej

Transakcje w sieci można dokonywać także za pomocą kart płatniczych. Podobnie jak w przypadku bankowości internetowej należy ignorować wszelkie wiadomości e-mail z prośbą o podanie numerów kart. Nie należy korzystać z mało znanych sklepów internetowych oraz ze sklepów, gdzie musimy podać dane na zwykłej, nie szyfrowanej stronie (brak https:// w adresie). W przypadku kart płatniczych newralgiczne dane to oprócz numeru kody CVV i CVV2 i PIN. Warto wiedzieć, że w placówkach BS Jarocin dostępne są specjalne karty przedpłacone do transakcji internetowych. Dla takiej karty zakładamy odrębny rachunek techniczny, który można zasilić odpowiednią kwotą tuż przed dokonaniem transakcji. Karta nie jest powiązana z kontem bankowym, czy limitem kredytowym, nie istnieją zatem obawy, że jeśli dane wpadną w ręce niepowołanych osób, stracimy więcej pieniędzy.

SYSTEM 3D SECURE

System 3D Secure posiada certyfikacje organizacji płatniczych VISA International oraz MasterCard International i umożliwia dokonywanie transakcji przez Internet o **zwiększonym stopniu bezpieczeństwa**. Klient każdą transakcję potwierdza dodatkowym hasłem, które nadaje sobie przy rejestracji karty w usłudze.