paysera

Jak bezpiecznie korzystać z usług Paysera?

System Paysera jest całkowicie bezpieczny, jednak bezpieczeństwo konta i danych zależy również od twoich działań w internecie. Poniższe zalecenia pomogą zapewnić bezpieczeństwo twoich działań na koncie Paysera i ogólnie w internecie.

Konto

Do systemu Paysera możesz zalogować się za pomocą aplikacji mobilnej (podając hasło lub logując się przy użyciu danych biometrycznych) lub za pomocą aplikacji w wersji na komputer.

Zaloguj się za pomocą aplikacji w wersji na komputer, wykonując następujące czynności:

1. Przejdź do https://www.paysera.com Kliknij *LOGOWANIE*, a zostaniesz przekierowany na stronę https://bank.paysera.com/pl/login.
2. Wybierz metodę identyfikacji – adres e-mail lub numer telefonu. Wprowadź wybrane dane.

3. Wybierz metodę logowania do konta:

- przez aplikację mobilną. Podczas logowania za jej pomocą konieczne będzie potwierdzenie kodu kontrolnego w aplikacji (musi być zgodny z kodem wyświetlanym w oknie przeglądarki). Otwórz aplikację Paysera i przesuń pasek potwierdzenia, jeśli kod wyświetlany na ekranie logowania jest zgodny z kodem w aplikacji. W celu zapewnienia większego bezpieczeństwa zalecamy używanie funkcji Touch ID lub Face ID do identyfikacji dostępu do aplikacj.
- podając hasło. Po wprowadzeniu hasła uzyskasz dostęp do swojego konta i możesz zobaczyć informacje o koncie, ale nie możesz korzystać z żadnych funkcji. Aby w pełni zarządzać swoim kontem, musisz potwierdzić logowanie: w górnym menu po lewej stronie dotknij *Potwierdzenie logowania* i wybierz

metodę – przez aplikację mobilną lub SMS. Pamiętaj, że usługa SMS wiąże się z dodatkowymi opłatami.

#

#

Podczas logowania do konta za pomocą aplikacji w wersji na komputer pamiętaj o kilku bardzo ważnych zasadach bezpieczeństwa:

- otwórz nowe okno przeglądarki i wprowadź adres https://www.paysera.x (zamiast x można wpisać tylko następujące domeny: **lt**, **com< /strong>, lv, bg, ee, pl, es, < strong>de**, **ro**, **al**, **ge**). W prawym górnym rogu kliknij Zaloguj się, a zostaniesz przekierowany na stronę https://bank.paysera.com/en/login. Upewnij się, że połączenie jest szyfrowane (kłódka jest widoczna, a adres zaczyna się od „https" – upewnij się, że na końcu znajduje się litera „s" – w niektórych przypadkach jest ona widoczna tylko po kliknięciu paska adresu), a dla zapewnienia bezpieczeństwa połączenia certyfikat elektroniczny został wydany tylko firmie Paysera, jak pokazano na ilustracji.

System Paysera nie jest dostępny pod żadnym innym, nawet i bardzo podobnym adresem internetowym, takim jak www.payssera.com, bank.paysera.anotherdomain.com, paysera.myf1ntech.com/paysera/login itp.

Jeśli pod tego rodzaju adresami trafisz na stronę, która jest bardzo podobna do oficjalnej strony Paysera, jest bardzo prawdopodobne, że znalazłeś się w pułapce przestępczej. W takim przypadku nie wprowadzaj żadnych danych i niezwłocznie powiadom Centrum Obsługi Klienta Paysera.

- zawsze wylogowuj się ze swojego konta. Unikaj logowania do konta na komputerach publicznych lub urządzeniach innych osób, ponieważ mogą one zawierać programy wykradające hasła lub inne dane.
- przynajmniej raz w miesiącu zalecamy sprawdzenie adresów IP, z których uzyskiwano dostęp do konta. Możesz to zrobić, klikając *Ustawienia > Ustawienia profilu > Historia logowania*. Jeśli masz podejrzenie, sprawdź, czy nie doszło do transakcji lub logowania z innego adresu IP. System umożliwia klientowi ustawienie na jego koncie adresów IP, z których możliwe będzie logowanie do konta klienta: *Ustawienia > Ustawienia profilu > Dodatkowe zabezpieczenia*. Jeśli coś podejrzewasz, natychmiast skontaktuj się z Centrum Obsługi Klienta.
- nie przekazuj nikomu danych logowania do konta. Jeśli ktoś zaoferował ci otwarcie konta Paysera w imieniu swoim lub innej osoby lub wykonanie czynności finansowych, skontaktuj się z Centrum Obsługi Klienta, a zostaniesz poinformowany o dalszych krokach.
- aktualizuj swoje dane osobowe i kontaktowe natychmiast, jeśli ulegną zmianie. W przypadku wystąpienia incydentów związanych z bezpieczeństwem lub w celu przekazania ci ważnych informacji, pracownicy Paysera mogą potrzebować natychmiastowego kontaktu z tobą lub przeprowadzenia odpowiedniej identyfikacji.
- nowo zarejestrowani klienci systemu Paysera powinni zwrócić uwagę na kwestionariusz KYC. Ilustracja po prawej stronie pokazuje, jak wygląda on w aplikacji mobilnej Paysera.

Przypominamy, że pracownicy Paysera, którzy się z Tobą skontaktowali, nigdy nie proszą o loginy, kody potwierdzające transakcje lub hasła. Pracownicy Paysera mogą zażądać pewnych danych do logowania tylko wtedy, gdy **sam zadzwonisz do** Centrum Obsługi Klienta i **tylko w celu identyfikacji**. Jeśli podejrzewasz, że mówi do Ciebie nie pracownik Paysera, poproś zadzwonić później i sam skontaktuj się z Centrum Obsługi Klienta Paysera.

#

Hasło konta

Hasło do konta musi być unikalne i składać się z co najmniej 8 znaków, wielkich i małych liter, cyfr i znaków specjalnych.

Nie używaj w haśle swoich danych osobowych ani informacji o członkach rodziny, na przykład daty urodzenia, imion lub nazwisk członków rodziny lub przyjaciół, imion zwierząt domowych lub cyfr i liter, które są łatwe do odgadnięcia.

Spróbuj zapamiętać hasło i nie przechowuj go w notatniku, telefonie ani w innym miejscu. Sugerujemy korzystanie z aplikacji do przechowywania haseł i przechowywanie hasła w postaci zaszyfrowanej.

Nie używaj tego samego hasła w innych systemach, ponieważ może ono również służyć do logowania się na twoje konto Paysera. Jeśli podejrzewasz, że inne osoby znają twoje hasło, zmień je natychmiast i sprawdź, czy nie doszło do nieautoryzowanego logowania do konta oraz czy nie miały miejsca żadne transakcje płatnicze lub próby ich wykonania.

Zalecamy zmianę hasła przynajmniej raz na 3-6 miesięcy.

Pamiętaj, **Paysera nie wysyła wiadomości z prośbą o zmianę hasła**. Nawet jeśli Paysera powiadomi Cię o zagrożeniach dla Twoich danych lub konta, lub powiadomi Cię o konieczności podjęcia jakichkolwiek działań, wiadomości nigdy nie będą zawierać **linku**, który po kliknięciu przekieruje klienta na stronę resetowania hasła. Ponadto Paysera nigdy **nie wymaga od klientów pobierania** załączonych plików, instalowania oprogramowania ani zgłaszania kodów dostępu. Po otrzymaniu podejrzanej wiadomości natychmiast powiadom Centrum Obsługi Klienta.

#

Urządzenia inteligentne

Używaj tylko tych urządzeń typu smart, które zostały legalnie nabyte i oficjalnie importowane, w których oprogramowanie systemu operacyjnego nie zostało zmodyfikowane (zhakowane) i na których nie zainstalowano aplikacji pochodzących ze źródeł innych niż Google Play i App Store.

Gdy urządzenie typu smart nie jest używane, należy je zablokować kodem, hasłem lub w inny sposób. Kod blokady urządzenia i kod PIN do aplikacji Paysera nie powinny stanowić części twojego numeru telefonu, tablic rejestracyjnych samochodu, dat urodzenia lub innych istotnych dla ciebie liczb – wszystkie kody muszą być unikalne oraz należy użyć funkcji Face ID lub Touch ID.

Oprogramowanie zainstalowane fabrycznie oraz inne aplikacje należy aktualizować natychmiast po ogłoszeniu wydania aktualizacji przez producenta oprogramowania. Aktualizacje producenta mają na celu nie tylko eliminację usterek, ale także łatanie luk w zabezpieczeniach, a to jeden z gwarantów bezpieczeństwa transakcji wykonywanych na twoim urządzeniu.

Na wszystkich urządzeniach, których używasz do łączenia się z kontem Paysera, zainstaluj oprogramowanie antywirusowe. Zalecamy również zainstalowanie zapory ogniowej, zwłaszcza na komputerach, ponieważ uniemożliwia to logowanie się do komputera z internetu.

#

Inne działania online

Zachowaj czujność, przesyłając swoje dane osobowe w środowisku internetowym – upewnij się, że podajesz je na zaufanej stronie internetowej.

Przed zrobieniem zakupów online sprawdź reputację sklepu na forach dla kupujących i na stronach z ocenami. Nowo zarejestrowana nazwa sklepu (domena), brak prawdziwej nazwy firmy, numeru rejestracyjnego i danych kontaktowych może świadczyć o niskiej wiarygodności sklepu. Zwróć również uwagę na adres witryny – czy zaczyna się od czegoś innego niż znaki http**s**:// i czy występuje litera „s”.

Podczas zakupów online często sugerowana jest płatność kartą i wymagane jest podanie danych karty. Kupuj tam, gdzie widoczne są specjalne logo potwierdzające bezpieczeństwo płatności: 3D Secure, Verified by Visa i Mastercard SecureCode.

Nie klikaj nieznanych lub zamaskowanych łączy internetowych, np. które zostały skrócone, nie ujawniają prawdziwego źródła, pojawiają się w sieciach społecznościowych lub są wysyłane przez wiadomość SMS lub e-mail. Nie otwieraj nieznanych dokumentów, nie instaluj oprogramowania z nieznanych źródeł i nie odwiedzaj niebezpiecznych stron internetowych.

#

#

Certyfikowane bezpieczeństwo

Bezpieczeństwo systemu Paysera potwierdza międzynarodowy standard technologii i procesów bezpieczeństwa PCI DSS (Payment Card Industry Data Security Standard). Ten standard bezpieczeństwa reguluje wymagania dla firm akceptujących płatności kartą i przetwarzających dane klientów. W systemie Paysera został zainstalowany najwyższy standard poziomu 1, przeznaczony do bezpiecznego przeprowadzania ponad 6 milionów transakcji kartowych rocznie.

#

W przypadku jakiejkolwiek podejrzanej sytuacji – jeśli otrzymasz podejrzaną wiadomość w imieniu Paysera, zauważysz podejrzane transakcje, zgubisz dane do logowania lub zorientujesz się, że wpisałeś je na fałszywej stronie internetowej itp., natychmiast skontaktuj się z Centrum Obsługi Klienta Paysera. Zawsze pomożemy Ci znaleźć wyjście!