

Kā droši izmantot Paysera pakalpojumus?

Paysera sistēma ir pilnīgi droša, tomēr konta un datu drošība ir atkarīga arī no jūsu darbībām internetā. Zemāk sniegtie ieteikumi palīdzēs uzturēt drošību jūsu darbībām Paysera kontā un internetā kopumā.

Konts

Paysera sistēmai varat pieslēgties mobilajā lietotnē (ievadot paroli vai izmantojot biometriskos datus) vai darbvirsmas versijā.

Pieslēdzieties kontam darbvirsmas versijā, veicot šādas darbības:

1. Ejiet uz <https://www.paysera.com>, spiediet *Pieslēgties* un jūs tiksiet novirzīts uz <https://bank.paysera.com/lv/login>.
2. Izvēlieties identifikācijas veidu – e-pasta adresi vai tālruņa numuru – un ievadiet to.
3. Izvēlieties pieslēgšanās veidu:
 - ar mobilo lietotni. Lai pieslēgtos, jums būs jāapstiprina kontroles kods lietotnē (tam jāatbilst kodam pārlūka logā). Atveriet Paysera lietotni un pavelciet apstiprinājuma joslu, ja ekrānā redzamais kods atbilst kodam lietotnē. Lielākai drošībai ieteicams izmantot Touch ID vai Face ID;
 - ievadot paroli. Pēc tās ievadīšanas jūs piekļūsiet savam kontam un varēsiet redzēt sava konta informāciju, taču nevarēsiet veikt nekādas darbības. Lai pilnībā pārvaldītu kontu, jums būs jāapstiprina pieslēgšanās: kreisajā augšējā stūrī noklikšķiniet uz “Papildu apstiprinājums” un izvēlieties veidu – ar mobilo lietotni vai īsziņu. Lūdzu ņemt vērā, ka SMS pakalpojumam tiek piemērota papildu maksa.

#

#

Lūdzu, ņemiet vērā vairākus ļoti svarīgus drošības noteikumus, pieslēdzoties kontam darbvirsmas versijā:

- atveriet jaunu pārākuma logu un ievadiet adresi <https://www.paysera.x> ("x" vietā var ievadīt tikai šādus domēnus: **lt, com, lv, bg, ee, pl, es, de, ro, al, ge**). Augšējā labajā stūrī noklikšķiniet uz *Pieslēgties*, un jūs tiksiet novirzīts uz <https://bank.paysera.com/lv/login>. Pārliecinieties, ka savienojums ir šifrēts (ir redzama atslēga un adrese sākas ar "https"; lūdzu, pārliecinieties, ka burti "s" ir novietoti beigās – dažos gadījumos tas ir redzams tikai tad, ja ir noklikšķināts uz adreses joslas). Drošam savienojumam elektronisko sertifikātu izsniedz tikai uzņēmumam Paysera, kā parādīts attēlā.

Paysera sistēma nav pieejama citās, pat ļoti līdzīgās vietņu adresēs, piemēram, www.payssera.com, bank.paysera.anotherdomain.com, paysera.myf1ntech.com/paysera/login u.c.

Ja ar šāda veida adresēm sasniedzāt vietni, kas ir ļoti līdzīga oficiālajai Paysera vietnei, ļoti iespējams, ka nonācāt noziedzīgā slazdā. Šajā gadījumā neievadiet nekādus datus un nekavējoties sazinieties ar [Paysera Klientu atbalsta centru](#).

- Vienmēr izrakstieties no sava konta. Izvairieties no pieslēgšanās kontam publiski pieejamos datoros vai citu personu ierīcēs, jo tajos var būt ļaunprātīga programmatūra, kas zog paroles vai citus datus.
- Iesakām vismaz reizi mēnesī pārbaudīt IP adreses, no kurām tika piekļūts jūsu kontam. To var izdarīt sadaļā *Iestatījumi > Profila iestatījumi > Pieslēgšanās vēsture*. Ja rodas aizdomas, pārbaudiet, vai nav bijuši darījumi vai pieslēgšanās no citām IP adreses. Sistēma ļauj klientam savā kontā iestatīt IP adreses, no kurām būs iespējama pieslēgšanās klienta kontam: *Iestatījumi > Profila iestatījumi > Papildu drošības līdzekļi*. Aizdomu gadījumā, lūdzu, nekavējoties sazinieties ar [Klientu atbalsta centru](#).
- Nevienam nepārsūtiet pieslēgšanās kontam datus. Ja kāds jums ir piedāvājis atvērt Paysera kontu savā vai citas personas vārdā vai veikt finanšu darbības, sazinieties ar Klientu atbalsta centru, un jūs tiksiet informēts par nākamajām darbībām.
- Nekavējoties atjauniniet savu personisko un kontaktinformāciju, ja tā mainās. Drošības incidentu gadījumā vai lai sniegtu jums svarīgu informāciju, Paysera darbiniekiem var nākties ar jums sazināties un/vai pienācīgi jūs identificēt.
- Paysera sistēmā nesen reģistrētām personām uzmanība jāpievērš Klienta anketai. Attēlā pa labi redzams, kā tā izskatās Paysera mobilajā lietotnē.

Lūdzu ņemt vērā, ka Paysera darbinieki, kuri ar jums sazināsies, nekad nelūgs atklāt pieslēgšanās datus vai darījuma apstiprināšanas kodus vai paroles. Paysera darbinieki var pieprasīt noteiktus pieslēgšanās datus tikai tad, ja jūs **pats zvanāt** uz Klientu atbalsta centru un **tikai personas identifikācijai**. Ja jums ir aizdomas, ka nerunājat ar Paysera darbinieku, palūdziet viņam vēlāk atzvanīt un sazinieties ar [Paysera Klientu atbalsta centru](#).

#

Konta parole

Konta parolei jābūt unikālai, un tajā jābūt vismaz 8 rakstzīmēm, lielajiem un mazajiem burtiem, cipariem un īpašajām rakstzīmēm.

Lūdzu, parolē neizmantojiet personisko vai ģimenes locekļu informāciju, piemēram, dzimšanas datumu, ģimenes locekļu vai draugu vārdus, uzvārdus, mājdzīvnieku vārdus, skaitļus un burtus, kurus var viegli uzminēt.

Lūdzu, mēģiniet atcerēties paroli un neglabājiet to piezīmju grāmatiņā, tālrunī vai citur. Mēs iesakām izmantot paroli glabāšanas lietotnes un glabāt savu paroli šifrētu.

Nelietojiet to pašu paroli citās sistēmās, jo tā var tikt izmantota, lai pieslēgtos jūsu Paysera kontam. Ja jums ir aizdomas, ka citas personas zina jūsu paroli, nekavējoties nomainiet to un pārbaudiet, vai nav bijuši neatļautas pieslēgšanās gadījumi un vai nav bijuši kādi faktiski vai plānoti neatļauti maksājumi.

Iesakām nomainīt paroli vismaz reizi 3-6 mēnešos.

Lūdzu ņemt vērā, ka **Paysera nesūta ziņojumus, kuros tiek lūgts mainīt paroli**. Pat ja Paysera informētu par draudiem jūsu datiem vai kontam vai par nepieciešamību veikt kādas darbības, ziņojumos **nekad nebūs saites** uz paroles mainīšanas lapu. Paysera arī **nekad neprasa, lai klienti lejupielādētu** pievienotos failus, instalētu programmatūru vai atklātu pieslēgšanās kodus. Pēc šāda ziņojuma saņemšanas, lūdzu, nekavējoties sazinieties ar [Klientu atbalsta centru](#).

#

Viedierīces

Izmantojiet tikai tās viedierīces, kuras ir likumīgi iegādātas un oficiāli importētas, kuru operētājsistēmas programmatūra nav modificēta (uzlauzta) un kurās nav instalētas lietotnes no citiem avotiem, nevis Google Play un App Store.

Ja viedierīce netiek izmantota, tā ir jābloķē ar kodu, paroli vai citiem līdzekļiem. Ierīces bloķēšanas kodam un Paysera lietotnes PIN kodam nevajadzētu sakrist ar jūsu tālruņa numura daļām, automašīnas numura zīmēm, dzimšanas datumiem vai citiem numuriem, kas attiecas uz jums – visiem kodiem jābūt unikāliem vai arī jāizmanto Face ID vai Touch ID.

Iepriekš instalētā un cita lietojumprogrammatūra ir jāatjaunina tūlīt pēc tam, kad programmatūras ražotājs ir paziņojis par atjauninājumiem. Ražotāja atjauninājumi ir paredzēti ne tikai darbības traucējumu novēršanai, bet arī drošības nepilnību novēršanai, un tie ir viena no drošības garantijām darbībām, ka tiek veiktas ar jūsu ierīci.

Visās ierīcēs, kuras izmantojat, lai pieslēgtos Paysera kontam, instalējiet antivīrusa programmatūru. Iesakām arī instalēt ugunsdmuri it īpaši datoros, jo tas neļautu pieslēgties datoram no interneta.

#

Citas darbības tiešsaistē

Esiet uzmanīgs, sniedzot savus personas datus tiešsaistē, pārliecinieties, vai attiecīgā vietne ir uzticama.

Pirms iepirkšanās tiešsaistē pārbaudiet veikalu reputāciju pircēju forumos un reitingu vietnēs. Nesen reģistrēts veikala nosaukums (domēns), uzņēmuma īstā vārda, reģistrācijas numura un kontaktinformācijas neesamība var norādīt uz veikala zemu uzticamību. Lūdzu, ņemiet vērā arī vietnes adresi – vai tā sākas ar **https://** un ir burts "s".

Iepērkoties tiešsaistē, bieži tiek ieteikti maksājumi ar karti un pieprasīti kartes dati. Iepērcieties tur, kur ir redzami īpaši logotipi, kas apstiprina maksājumu drošību: 3D Secure, Verified by Visa un MasterCard SecureCode.

Neklikšķiniet uz nezināmām vai maskētām saitēm, piemēram, saīsinātām, kas neatklāj patieso avotu, parādās sociālajos tīklos vai tiek nosūtītas īsziņā vai e-pastā. Neatveriet nezināmus dokumentus, neinstalējiet programmatūru no nezināmiem avotiem, neapmeklējiet nedrošas vietnes.

#

#

Sertificēta drošība

Paysera sistēmas drošību apstiprina starptautiskais drošības tehnoloģiju un procesu standarts PCI DSS (Payment Card Industry Data Security Standard). Šis drošības standarts regulē prasības uzņēmumiem, kas pieņem karšu maksājumus un apstrādā klienta datus. Paysera sistēmā ir uzstādīts augstākais 1. līmeņa standarts, kas paredzēts drošai vairāk nekā 6 miljonu karšu darījumu gadā veikšanai.

#

Aizdomīgu situāciju gadījumā – aizdomīgs ziņojums Paysera vārdā, aizdomīgi darījumi, pieslēgšanās datu zudums vai datu ievadīšana viltus vietnē u.c. – lūdzu, nekavējoties sazinieties ar Paysera Klientu atbalsta centru. Mēs vienmēr palīdzēsim jums rast risinājumu!