Kaip saugiai naudotis Paysera paslaugomis?

Paysera sistema yra visiškai saugi, tačiau dalis jūsų paskyros ir duomenų saugumo priklauso nuo jūsų atliekamų veiksmų internete. Žemiau pateikiame rekomendacijas, kurios padės užtikrinti jūsų atliekamų veiksmų Paysera paskyroje bei bendrai internetinėje erdvėje saugumą.

Paskyra

Prie Paysera sistemos galima prisijungti per mobiliąją programėlę (suvedant slaptažodį, jungiantis su piršto antspaudu (Touch ID) ar veido atpažinimo sistema (Face ID)) arba per elektroninę bankininkystę.

Prisijungimas per elektroninę bankininkystę vyksta keliais žingsniais:

1. Eikite į https://www.paysera.lt, spauskite *Prisijungimas*, ir būsite nukreipti į https://bank.paysera.com/lt/login.
2. Pasirinkite, kaip patvirtinsite savo tapatybę – naudojant elektroninio pašto adresą ar telefono numerį. Suveskite prašomus duomenis.

3. Pasirinkite būdą, kuriuo norite jungtis prie paskyros:

- naudojant mobiliąją programėlę. Jungiantis turėsite programėlėje patvirtinti kontrolinį kodą (jis turi sutapti su kodu, rodomu naršyklės lange). Rekomenduojame programėlėje atpažinimui naudoti biometrinius duomenis – pirštų antspaudus ar veido atpažinimo sistemą, taip užtikrinant didesnį saugumą.
- naudojant slaptažodį. Jį suvedus būsite prijungtas prie savo paskyros, matysite sąskaitos informaciją, tačiau negalėsite naudotis visomis paslaugomis. Norint pilnai valdyti paskyrą, turėsite patvirtinti prisijungimą: meniu viršuje kairėje spauskite *Prisijungimo patvirtinimas* ir pasirinkite, kuriuo būdu norite atlikti šį veiksmą – per mobiliąją programėlę ar SMS žinute. Atkreipkite dėmesį, kad SMS siuntimui taikomas papildomas mokestis.

#

#

Prie paskyros jungiantis per elektroninę bankininkystę, reikėtų nepamiršti kelių saugai labai svarbių taisyklių:

- atidarykite naują naršyklės langą ir įveskite adresą https://www.paysera.x (x vietoje gali būti tik šie domenai: **lt**, **com**, **lv**, **bg**, **ee**, **pl**, **es**, **de**, **ro**, **al**, **ge**). Dešiniajame viršutiniame kampe spauskite Prisijungti ir būsite nukreipti į https://bank.paysera.com/lt/login. Įsitikinkite, kad ryšys yra šifruojamas (matoma spynelė ir adresas prasideda „https“ – atkreipkite dėmesį, kad gale būtinai būti raidelė „s“ – kai kuriuose naršyklėse matomas tik paspaudus adreso įvedimo eilutę), o saugiam ryšiui naudojamas tik Paysera bendrovei išduotas elektroninis sertifikatas, kaip tai parodyta paveikslėlyje.

Kitokiu, kad ir labai panašiu svetainės adresu, pvz., www.payssera.com, bank.paysera.anotherdomain.com, paysera.myf1ntech.com/paysera/login ir pan., Paysera sistema nėra pasiekiama.

Jei tokiu adresu pasiekėte svetainę, kuri yra labai panaši į oficialią Paysera svetainę, greičiausiai, pakliuvote į sukčių spąstus. Tokiu atveju neįvedinėkite jokių duomenų ir nedelsiant informuokite Paysera Klientų aptarnavimo centrą.

- visada atsijunkite nuo savo paskyros. Venkite prie paskyros jungtis naudojantis viešaisiais kompiuteriais ar kitų asmenų įrenginiais, nes juose gali būti slaptažodžius ar kitus duomenis vagiančių programų.
- rekomenduojame bent kartą per mėnesį patikrinti IP adresus, iš kurių buvo jungtasi prie jūsų paskyros. Tai galite padaryti kairiajame meniu (apačioje) paspaudę *Nustatymai > Paskyros nustatymai > Prisijungimų istorija*. Jeigu kilo įtarimas, pasitikrinkite, ar nebuvo ne jūsų atliktų operacijų, prisijungimų iš svetimo IP adreso. Sistema leidžia klientui savo paskyroje nustatyti IP adresus, iš kurių bus leidžiama prisijungti prie jo sąskaitos: *Nustatymai > Paskyros nustatymai > Papildomo saugumo priemonė*. Kylant įtarimui, nedelsiant susisiekite su Klientų aptarnavimo centru.
- niekam neperduokite prisijungimo prie paskyros duomenų. Jei kas nors jums pasiūlė savo ar kito asmens vardu atidaryti Paysera paskyrą ar atlikti finansinius veiksmus, susisiekite su Klientų aptarnavimo centru, ir specialistai patars, kaip elgtis toliau.
- atnaujinkite savo asmeninę informaciją ir kontaktus, kai tik jie pasikeičia. Įvykus saugos incidentams ar siekiant jums suteikti svarbios informacijos, Paysera darbuotojams gali prireikti nedelsiant su jumis susisiekti ir (arba) jus tinkamai identifikuoti.
- naujai Paysera sistemoje besiregistruojantiems asmenims būtina atkreipti dėmesį į kliento pažinimo (KYC) anketą. Ji Paysera programėlėje atrodo kaip parodyta paveikslėlyje dešinėje.

Primename, kad su jumis susisiekę Paysera darbuotojai niekuomet neprašo pasakyti prisijungimo ar operacijų patvirtinimo kodų, slaptažodžių. Tam tikrų prisijungimo duomenų Paysera darbuotojai gali paprašyti tik tuo atveju, jei jūs **pats skambinsite** į Klientų aptarnavimo centrą ir **tik asmens tapatybės identifikavimo tikslu**. Kilus įtarimui, kad su jumis kalba ne Paysera darbuotojas, paprašykite paskambinti jums vėliau, o patys susisiekite su Paysera Klientų aptarnavimo centru.

#

Paskyros slaptažodis

Prisijungimo prie paskyros slaptažodis turi būti unikalus, sudarytas iš ne mažiau kaip 8 simbolių, naudojant didžiąsias ir mažąsias raides, skaičius bei specialiuosius simbolius.

Slaptažodyje nenaudokite informacijos apie save ar savo šeimos narius, pavyzdžiui, gimimo datos, šeimos narių ar draugų vardų, pavardžių, gyvūnų vardų, lengvai atspėjamų skaičių ir raidžių kombinacijų.

Pasistenkite įsiminti slaptažodį ir nelaikyti jo užrašyto užrašų knygelėje, telefone ar kitur. Patariame naudotis slaptažodžių saugojimui skirtomis programomis ir slaptažodį laikyti užšifruotą.

Nenaudokite to paties slaptažodžio kitose sistemose, nes jis gali būti panaudotas ir jungiantis prie jūsų Paysera paskyros. Kilus įtarimams, kad slaptažodis galėjo tapti žinomas kitiems asmenims, nedelsiant jį pasikeiskite ir patikrinkite, ar nebuvo neteisėtų prisijungimų prie paskyros ar įvykdytų arba bandytų įvykdyti neteisėtų mokėjimo operacijų.

Rekomenduojame slaptažodį keisti ne rečiau kaip kas 3-6 mėn.

Atminkite, **Paysera nesiunčia pranešimų reikalaudama pasikeisti slaptažodį**. Net jeigu Paysera informuotų apie grėsmes jūsų duomenims ar paskyrai, ar praneštų apie poreikį atlikti kokius nors veiksmus, žinutėse niekada **nebus nuorodos**, kurią paspaudęs klientas būtų peradresuojamas į slaptažodžio keitimo puslapį. Taip pat Paysera niekada **nereikalauja klientų parsisiųsti** prisegtų failų, įsidiegti programinės įrangos ar pranešti prisijungimo kodus. Gavus įtartiną pranešimą, prašome nedelsiant informuoti Klientų aptarnavimo centrą.

#

Išmanieji įrenginiai

Naudokitės tik legaliai įgytais ir oficialiai į Lietuvą importuotais išmaniaisiais įrenginiais, kuriuose nėra pakeista (nulaužta) operacinės sistemos programinė įranga ir iš nepatikimų šaltinių ar kitų nei „Google Play“ ir „Apple Store“ parduotuvių įdiegta taikomoji programinė įranga.

Kai išmanusis įrenginys nėra naudojamas, jis turėtų būti užrakintas kodu, slaptažodžiu ar kita priemone. Tiek įrenginio, tiek Paysera programėlės užrakto kodas neturi sutapti su jūsų telefono ar automobilio numeriu, artimųjų gimtadienių datomis ar kitomis jums artimomis ir lengvai nuspėjamomis skaičių sekomis – naudokite tik unikalias skaičių kombinacijas s arba pasitelkite pirštо antspaudo, veido atpažinimo ar kita išmaniąją technologiją.

Įrenginio gamyklinė ir taikomoji programinė įranga turėtų būti atnaujinama, kai tik programinės įrangos gamintojas praneša apie išleistą naujinių paketą. Gamintojas naujiniais ne tik šalina pastebėtus trikdžius, bet tuo pat metu lopo saugos spragas, o tai yra viena iš jūsų įrenginiu vykdomų operacijų saugumo garantijų.

Visuose įrenginiuose, kuriais jungiatės prie Paysera paskyros, įsidiekite antivirusinę programą. Taip pat kompiuteriuose rekomenduojame įsidiegti ugniasienę (angl. *firewall*), kuri neleistų prisijungimo prie įrenginio iš interneto.

#

Kiti veiksmai internete

Būkite budrūs pateikdami savo asmeninius duomenis internetinėje erdvėje – įsitikinkite, kad juos pateikiate patikimoje svetainėje.

Prieš pirkdami internete, patikrinkite parduotuvių reputaciją pirkėjų forumuose ir reitingus pateikiančiose svetainėse. Žemą parduotuvės patikimumą gali išduoti ką tik užregistruotas parduotuvės vardas (domenas), svetainėje nenurodytas įmonės tikrasis pavadinimas ir registracijos numeris, kontaktinės informacijos nebuvimas. Atkreipkite dėmesį ir į svetainės adresą – ar jis neprasideda kitais nei https:// simboliais, ar yra raidelė „s“.

Perkant elektroninėse parduotuvėse dažnai siūloma atsiskaityti mokėjimo kortele, nurodant jos duomenis. Ieškokite atliekamų mokėjimų saugumą patvirtinančių specialių logotipų: „3D Secure“, „Verified by Visa“ ir „Mastercard SecureCode“.

Nespauskite socialiniuose tinkluose, SMS žinutėse bei elektroniniuose laiškuose atsiųstų nežinomų ar užmaskuotų, pvz., sutrumpintų, neatskleidžiančių tikrojo šaltinio, interneto nuorodų, neatidarinėkite nežinomų dokumentų, nediekite programinės įrangos iš nežinomų šaltinių, nesilankykite nesaugiuose tinklapiuose.

#

#

Sertifikuotas saugumas

Paysera sistemos saugumą patvirtina tarptautinis saugumo technologijų ir procesų standartas PCI DSS (angl. Payment Card Industry Data Security Standard). Šis saugumo standartas reglamentuoja reikalavimus bendrovėms, priimančioms atsiskaitymus kortelėmis ir tvarkančioms klientų duomenis. Paysera sistemoje įdiegtas aukščiausias – 1 lygio standartas, skirtas saugiai atlikti daugiau nei 6 mln. operacijų kortelėmis per metus.

#

Susidūrus su bet kokia įtarimą keliančia situacija – sulaukus Paysera vardu įtartinos žinutės, pastebėjus įtartinas operacijas, praradus prisijungimo duomenis ar supratus, kad juos įvedėte netikroje svetainėje ir pan., nedelsdami susisiekite su Paysera Klientų aptarnavimo centru. Mes visuomet padėsime rasti išeitį!