Kuidas Paysera teenuseid turvaliselt kasutada?

Paysera süsteem on täiesti turvaline, kuid konto ja andmete turvalisus oleneb ka teie tegevusest internetis. Allpool toodud soovitused aitavad tagada teie Paysera kontol ja üldiselt Internetis tehtavate toimingute turvalisuse.

Konto

Paysera süsteemi saate sisse logida mobiilirakenduse (sisestades parooli või logides sisse biomeetriliste andmetega) või veebiversiooni kaudu.

Logige sisse veebiversiooni, toimides järgnevalt:

1. Minge lehele https://www.paysera.com vajutage *Sisselogimine* ja teid suunatakse lehele https://bank.paysera.com/et/login.
2. Valige tuvastamisviis – e-posti aadress või telefoninuber. Ja sisestage andmed.

3. Valige konto sisselogimisviis:

- mobiilirakenduse kaudu. Kui kasutate seda sisselogimiseks, peate rakenduses kontrollkoodi kinnitama (see peab vastama veebilehitsejas kuvatud koodile). Avage Paysera rakendus ja libistage kinnitusriba, kui sisselogimisekraanil kuvatav kood vastab rakenduses oleva koodiga. Rakenduses juurdepääsu kinnitamiseks on soovitatav kasutada Touch ID'd või Face ID'd, et tagada suurem turvalisus.
- sisestades parooli. Pärast selle sisestamist pääsete oma kontole ja näete konto andmeid, kuid ei saa ühtegi toimingut teostada. Oma konto täielikuks haldamiseks peate sisselogimise kinnitama: vajutage vasakul lehe ülaosas “Sisselogimise kinnitus” ja valige meetod – mobiilirakenduse või SMS. Pange tähele, et SMS-teenuse kasutamisel rakendatakse lisatasusid.

#

#

Palun võtke arvesse mitut väga olulist turvareeglit, kui logite oma kontole veebiversiooni kaudu:

- avage uus veebilehitseja aken ja sisestage aadress https://www.paysera.x (x-i asemel võib olla sisestatud ainult järgmised domeenid: **lt**, **com**, **lv**, **bg**, **ee**, **pl**, **es**, **de**, **ro**, **al**, **ge**). Paremal üleval nurgas vajutage Sisselogimine ja teid suunatakse lehele https://bank.paysera.com/et/login. MVeenduge, et ühendus oleks krüpteeritud (lukk on nähtav ja aadress algab “https”, veenduge, et täht „s” oleks asetatud lõppu - mõnel juhul on see nähtav ainult siis, kui vajutatakse aadressiribale), ja turvalise ühenduse jaoks elektrooniline sertifikaat on väljastatud ainult Paysera ettevõttele, nagu on kuvatud pildil.

Paysera süsteem ei ole juurdepääsetav muudelt, isegi väga sarnastelt veebiaadressitelt, nt.: www.payssera.com, bank.paysera.muudomeen.com, paysera.myf1ntech.com/paysera/login jne.

Kui seda tüüpi aadressidel jõuate lehele, mis on väga sarnane Paysera ametliku veebilehega, on väga tõenäoline, et olete langenud kriminaalsesse lõksu. Sel juhul ärge sisestage andmeid teavitage koheselt Paysera Klienditeenindust.

- logige alati oma kontolt välja. Vältige oma kontole sisselogimist avalikest arvutitest või teiste inimeste seadmetest, kuna need võivad sisaldada pahavara, mis varastavad paroole või muid andmeid.
- soovitame vähemalt kord kuus kontrollida IP-aadresse, millelt teie kontole sisse logiti.. Seda saate teha oma kontol valides vasakult menüüst Seadistused > Paysera konto seadistused > Sisselogimisajalugu. Kui teil on kahtlusi, kontrollige, kas teistelt IP-aadressitelt oli tehtud mingeid tehinguid või sisselogimisi. Süsteem võimaldab kliendil seadistada IP-aadressid, millele kaudu on võimalik kontole sisselogida: Seadistused > Paysera konto seadistused > Täiendav turvameede. Kahtluste korral kontakteeruge koheselt Klienditoega.
- ärge edastage oma konto sisselogimisandmeid mitte kellelegi. Kui keegi on pakkunud teile, et avada nende või kolmanda isiku nimel Paysera konto või teostada rahalisi toiminguid, võtke koheselt ühendust Klienditoega ja teile antakse nõu järgnevate sammude asjus.
- uuendage koheselt oma isiklikke ja kontaktandmeid, kui need muutuvad. Turvaintsidentide korral või teile olulise teabe edastamiseks võivad Paysera töötajad vajada teiega viivitamatut ühendust võtta ja/või et teid korrektselt tuvastada.
- äsja Paysera süsteemis registreerunud isikud peaksid tähelepanu pöörama KYC küsimustikule. Parempoolsel pildil on kujutatud, kuidas see Paysera süsteemis välja näeb.

Pange tähele, et teiega ühendust võtavad Paysera töötajad ei palu teil kunagi oma sisselogimisandmeid, tehingu kinnituskoode või paroole avaldada. Paysera töötajad võivad teatud sisselogimisandmeid küsida ainult siis, kui teie **ise helistate** tKlienditoele ja **ainult Teie isiku tuvastamiseks**. Kui kahtlustate, et te ei räägi Paysera töötajaga, paluge tal hiljem teile uuesti helistada ja võtke ise ühendust Paysera Klienditoega.

#

Konto parool

Konto parool peab olema unikaalne ja koosnema vähemalt kaheksast tähemärgist, sisaldama suur- ja väiketähti, numbreid ja erisümboleid.

Ärge palun kasutage paroolis oma isiklikke ega pereliikmete andmeid, näiteks sünniaegu, sõprade või pereliikmete ees- või perekonnanimesid, lemmikloomade nimesid ega numbrid ja tähti, mida võib olla lihtne ära arvata.

Proovige parool meelde jätta ning ärge hoidke seda oma märkmikus, telefonis ega mujal. Soovitame kasutada paroolide salvestamisel rakendusi mis hoiavad teie parooli krüpteerituna.

Ärge kasutage sama parooli teistes süsteemides, sest seda võidakse kasutada ka teie Paysera kontole sisselogimiseks. Kui kahtlustate, et teised inimesed võivad teada teie parooli, muutke seda koheselt ja kontrollige, kas kontole on teostatud volitamata sisselogimisi või kas kontolt on teostatud või proovitud teostada tehinguid.

Soovitame parooli vahetada vähemalt iga 3–6 kuu tagant.

Pöörake tähelepanu, et **Paysera ei saada ühtegi teadet paludes teil parooli muuta**. Isegi kui Paysera teavitas teid teie andmeid või kontot ähvardavatest ohtudest või toimingute tegemise vajadusest, **ei sisalda teated kunagi linki** lehele, kus saab parooli vahetada. Samuti ei nõua Paysera **oma klientidel kunagi alla laadida** lisatud faile, insatallida tarkvara või avalikustada sisselogimiskoode. Pärast sellise teate saamist teavitage sellest viivitamatult Kliendituge.

#

Nutiseadmed

Kasutage ainult nutiseadmeid, mis on seaduslikult omandatud ja teie riiki ametlikult imporditud, mille operatsioonisüsteemi pole muudetud (häkitud) ja millele pole installitud rakendusi muudest allikatest kui Google Play ja App Store.

Kui nutiseadet ei kasutata, tuleb see lukustada koodiga, parooliga või muul viisil. Seadme ja Paysera rakenduse PIN-kood ei tohiks kokku langeda teie telefoninumbri, auto numbrimärgi, sünnikuupäevade või muude teie jaoks oluliste numbritega – kõik koodid peavad olema unikaalsed ja võimalusel tuleks kasutada Face ID'd või Touch ID'd.

Eelinstalleeritud ja muude rakenduste tarkvara tuleb värskendada kohe pärast värskenduste väljastamist tarkvaratootja poolt. Tootja värskendused ei ole mõeldud ainult rikete kõrvaldamiseks, vaid ka turvaaukude parandamiseks ja see on üks viis turvalisuse tagamiseks oma seadmega toimingute tegemisel.

Installige viirusetõrje kõigile seadmetele, mida kasutate Paysera kontole logimiseks. Samuti soovitame installida tulemüüri, eriti arvutitesse, kuna see takistab arvutisse sisselogimise internetist .

#

Muud tegevused veebis

Olge oma isikuandmete veebis edastamisel ettevaatlik ja veenduge, et andmeid esitades teeksite seda usaldusväärsel veebisaidil.

Enne veebis ostlemist kontrollige kaupluste mainet foorumitest ja veebisaitide reitingut. Äsja registreeritud kaupluse nimi (domeen), ettevõtte pärisnime, registreerimisnumbri ja kontaktandmete puudumine võib viidata kaupluse madalale usaldusväärsusele. Pange tähele ka veebisaidi aadressi – kui see algab millegi muuga kui http**s**:// ja kas täht “s” on olemas.

Interneti kaudu ostes soovitatakse sageli kaardimakseid teha mille jaoks nõutakse kaardi andmeid. Ostke sealt, kus on olemas spetsiaalsed maksete turvalisust kinnitavad logod: 3D Secure, Verified by Visa ja MasterCard SecureCode.

Ärge vajutage linkidel, mis on tundmatud või maskeeritud, nt. lühendatud, ei avalikusta tegelikku allikat, kuvatakse sotsiaalvõrgustikus või saadetakse SMS-i või e-posti teel. Ärge avage tundmatuid dokumente, ärge installige tarkvara tundmatutest allikatest ega külastage ohtlikke veebisaite.

#

#

Sertifitseeritud turvalisus

Paysera süsteemi turvalisust kinnitab rahvusvaheline andmeturbetehnoloogiate ja -protsesside standard PCI DSS (Payment Card Industry Data Security Standard). See turbestandard reguleerib kaardimakseid vastuvõtvate ja kliendiandmeid töötlevate ettevõtetele kehtestatud nõudeid. Paysera süsteemi on paigaldatud standardi kõrgeim 1. tase, mis on ette nähtud üle 6 miljoni kaarditehingu turvaliseks teostamiseks aastas.

#

Mis tahes kahtlaste olukordade puhul: kahtlane kiri Payseralt, kahtlased tehingud, sisselogimisandmete kadumine või andmete sisestamine valele veebisaidile jne.,pöörduge palun koheselt Paysera Klienditoe poole. Aitame teil alati lahenduse leida!