Mängukonto turvalisus algab e-postist: viis seadistust, mis tasub üle vaadata

8 min tagasi - 24.11.2026 Autor: AM

(Sisuturundus)

Mängija avab pärast pikemat pausi oma vana konto. Parool on alles, kuid kinnituskood saadetakse e-posti aadressile, mida ta pole aastaid kasutanud. Postkastile ligipääsu taastamine võtab nüüd rohkem aega kui mängukontole sisselogimine.

Sellise olukorra vältimiseks tasub aeg-ajalt vaadata üle viis seadistust. Need puudutavad e-posti, paroole, lisakinnitust, taastamisvõimalusi ja kontoga seotud seadmeid.

Ka veebikasiino konto sõltub e-postist

Mängukeskkonnad kasutavad e-posti registreerimisel, maksete kinnitamisel ja kontoandmete muutmisel. Seetõttu tuleks postkasti turvalisusele pöörata vähemalt sama palju tähelepanu kui mängukonto paroolile.

Välismaistel mänguplatvormidel võivad registreerimise ja isikusamasuse kontrollimise nõuded erineda. Läti turule suunatud välismaiste veebikasiinode ülevaade aadressil akazino.com/arzemju-kazino käsitleb näiteks konto loomist, makseviise ja kasutajate tuvastamist. Konto turvaseadistused tuleb siiski üle kontrollida valitud teenuse enda lehel.

E-posti kaudu saabuvad sageli ka parooli muutmise lingid. Kui keegi pääseb postkasti sisse, võib ta proovida taastada ligipääsu sellega seotud teenustele.

Esimene mõistlik samm on vaadata postkasti viimaseid sisselogimisi. Samuti tasub kontrollida, kas taastamiseks märgitud telefoninumber ja varuaadress veel töötavad.

Mõnes postkastis saab määrata ka teavitused tundmatust seadmest sisselogimise kohta. Kui selline kiri saabub, tasub kontrollida sisselogimise aega ja asukohta. Eriti kasulik on see juhul, kui sama e-posti aadressiga on seotud mitu mängukontot.

Üks parool ei peaks avama mitut kontot

Mängukonto parool võib olla loodud aastaid tagasi. Kui sama kombinatsioon on kasutusel veel e-postis ja mõnes veebipoes, tuleks see välja vahetada.

Riigi Infosüsteemi Amet soovitab oma kontode turvalisuse juhendis kasutada vähemalt 15 märgist koosnevaid paroole. Juhendis soovitatakse ka eri kontode jaoks erinevaid paroole ning paroolihalduri kasutamist.

Paroolihaldur võimaldab luua pika juhusliku parooli, mida ei pea meelde jätma. Salvestatud andmed leiab vajaduse korral rakendusest. Kui korraga on kasutusel mitu mängukontot, võib turvaseadistuste kontrollimisel alustada kolmest kohast:

- E-posti konto. Kontrolli parooli, taastamisaadressi ja kaheastmelise autentimise olemasolu.
- Mängukonto. Vaata üle sisselogimismeetod, seotud seadmed ja kontaktandmed.
- Paroolihaldur. Veendu, et selle põhiparool on tugev ning varukoopiale ligipääs olemas.

Kõigepealt tasub korda teha peamine e-postkast. Selle kaudu võib toimuda mitme teise konto taastamine. Seejärel saab mängukeskkondades vanad paroolid ükshaaval asendada.

Paroolihalduri seadistamisel tuleb hoolikalt valida põhiparool. Samuti on kasulik tutvuda sellega, kuidas teenus võimaldab ligipääsu taastada.

Kuhu läheb kuuekohaline kinnituskood?

Kaheastmeline autentimine lisab sisselogimisele teise kontrolli. Tavaliselt sisestab kasutaja esmalt parooli ning kinnitab seejärel oma isiku telefonis.

Mõnes teenuses saabub kuuekohaline kood SMS-iga. Teistes kasutatakse autentimisrakendust, mis loob regulaarselt uue koodi. Saadaval võib olla ka pääsukoodiga ehk passkey'ga sisselogimine.

Mõttekoja Praxis 2025. aasta uuring Eesti elanike küberturvalise käitumise kohta leidis, et inimesed rakendavad turvateadmisi sageli valikuliselt. Eriti tähelepanelikud ollakse internetipangas ja veebipoodides. Uuringus nimetati probleemidena ka nõrku paroole ning kaheastmelise autentimise vältimist.

Mängukonto puhul tasub lisakinnitus sisse lülitada kohe, kui teenus seda võimaldab. Autentimisrakendust vahetades tuleb enne vana telefoni kustutamist kontrollida, kuidas kontod uude seadmesse üle tuua.

Taastamiskoodid on mõeldud päris olukordadeks

Telefon võib kaduda, puruneda või jääda tehasesätete taastamise järel tühjaks. Kui sisselogimine sõltub ainult ühes seadmes olevast autentimisrakendusest, muutub konto taastamine keerulisemaks.

Mõned teenused annavad kaheastmelise autentimise aktiveerimisel ühekordsed varukoodid. Need tuleb salvestada kohta, kuhu pääseb ka ilma tavapärase telefonita. Enne uue seadme kasutuselevõttu võiks läbi teha järgmise kontrolli:

1. Varukoodide asukoht. Kontrolli, kas koodid on alles ja loetavad.
2. Taastamise kontaktandmed. Vaata, kas vana telefoninumber või e-post vajab asendamist.
3. Autentimisrakenduse üleviimine. Uuri, kas rakendus toetab kontode turvalist ülekandmist teise seadmesse.

Varukoode ei tohiks hoida tavalise ekraanipildina avalikult sünkroonitavas fotokaustas. Sobivam on krüpteeritud hoidla või turvalises kohas säilitatav paberkoopia.

Kui teenus pakub mitut taastamismeetodit, tasub nende tingimused läbi lugeda. Mõnikord on konto taastamiseks vaja kinnitada isikusamasust või esitada täiendavaid andmeid.

Vana sülearvuti võib endiselt sisse logitud olla

Mängukonto turvaseadetes võib leiduda aktiivsete seansside või usaldatud seadmete loend. Seal tasub kontrollida, kas konto on avatud mõnes ammu kasutamata arvutis.

Näiteks võib vana sülearvuti jääda pärast uue ostmist mitmeks kuuks kappi. Kui selle brauseris on mängukonto endiselt aktiivne, võiks seansi kaugelt lõpetada.

Kasutamata seadmete eemaldamine võtab tavaliselt vähe aega. Mõnes keskkonnas saab korraga välja logida kõigist seadmetest, teistes tuleb seansid eraldi sulgeda.

Kui kasutaja on mängukontole sisse loginud sõbra arvutist, tasub seanss pärast kasutamist lõpetada. Brauserisse salvestatud paroolid ja automaatne sisselogimine vajavad samuti tähelepanu. Avalikus arvutis tuleks hoiduda sisselogimisandmete salvestamisest.

Selline ülevaatus sobib hästi kokku parooli vahetamisega. Kui kontaktandmed, taastamisvõimalused ja aktiivsed seansid on korras, on mängukontot ka hiljem märksa lihtsam hallata.

- Uudised
- Sisuturundus

Pilt

