

Maksepettuste Ülevaade



Eesti Pank
EUROSÜSTEEM

2026

Eesti Panga kord aastas ilmuv Maksepettuste Ülevaade võtab kokku eelneval aastal tehtud maksepettuste statistika, levinud petuskeemid ja peamised pettuste tõkestamise meetmed.

Maksepettuste Ülevaadet saab lugeda Eesti Panga veebilehel.

Koostanud Eesti Pank, Eesti Pangaliit, Politsei- ja Piirivalveamet, Rahandusministeerium

Võrguväljaanne ISSN 3059-8346

Toimetanud Villu Känd

Kujundanud Urmas Raidma

SISUKORD

ÜLEVAADE EESTIS TEHTUD PETTUSTEST	4
PETTUSELIIGID	4
Autoriseeritud maksed (<i>authorised push payments</i> , APP).....	4
Andmepüük, kontode üle võtmised ja identiteedivargus	5
Kaardipettused	5
NÄITED AKTUAALSETEST PETTUSTEST	6
Maksejuhise muutmine ehk arvepettus (äriühingud)	6
Investeeringispettused	6
Mitmeastmelised kõnepettused	6
Kulleriskeemid	7
PETTUSTE ALGATAMISE VIISID.....	8
Maksekorralduspettused	8
Kaardipettused	10
Ettevõtetega seotud pettused	11
PETTUSTE STATISTIKA.....	13
Pettuste käive ja tehingute arv.....	13
Pettuste liigid	13
Pettuste keskmised kahjusummad.....	16
PETTUSED ERI PIIRKONDADES	18
Kaardipettused Eesti pangakaartidega	18
Maksekorralduspettused Eesti pangakontodelt.....	18
MAKSEPETTUSTE TÕKESTAMINE EESTIS	20
Finantspettuste tõkestamise ümarlaud	21
Olulisemad tegevused ja saavutused ümarlaua tegevuskava elluviimisel ning ümarlaua osalejate algatatud tegevused.	21
Inimene kui peamine pettuste tõkestaja	23

ÜLEVAADE EESTIS TEHTUD PETTUSTEST

2025. aasta tõi kaasa uue maksepettuste laine, mille tekitatud kahju oli varasemast märksa suurem, samas kui pettuste arv kasvas väiksemal määral. Suurima kahju põhjustasid endiselt maksekorralduspettused, millest levinumad olid investeerimispettused ja mitmeastmelised kõnepettused. Viimaste puhul esinesid petturid eraettevõtte või avaliku asutuse töötajana, näiteks kullerfirma või mobiilsideoperaatori esindaja, pangatöötaja või politseinikuna. Näiliste teenuste ja kontrollitoimingutega püüdsid nad ohvreid segadusse ajada ja nende usaldust võita. Enamasti kaotasid ohvrid raha ise petturitele ülekandeid tehes. Kolmandikul juhtudest said kurjategijad aga ligipääsu ohvri kontodele, mis võimaldas neil seal olevat raha liigutada ja ohvri nimel laenu võtta. Eriti aktiivselt sihiti väikeettevõtteid ning nende raamatupidajaid ja omanikke, et saada ligipääs nii erasiku kui ka ettevõtte kontole. Samuti pandi toime arvepettusi. Kaardipettustes on üha enam hakanud levima sularaha-, täpsemalt sularahaautomaadipettused. Kelmid püüavad veenda ohvreid panema pangakaarti koos PIN-koodiga pakiautomaati või võtma sularaha välja ja andma selle koduuksel rahakullerile. Pangaautomaadipettustest on nüüdseks saanud kaardipettuste peamine liik ja nende tekitatud kahju ületab juba e-kaubandusega seotud kaardipettuste kahju.

PETTUSELIIGID

Autoriseeritud maksed (authorised push payments, APP)¹

- **Müügipettus.** Kannatanu ostab internetipoest või järelturuplatvormilt kauba või teenuse, kuid „müüja“ kaob kohe pärast makse laekumist kaupa saatmata või teenust osutamata.
- **Investeerimispettus.** Ohvreid meelitatakse lubadusega teenida investeringutelt suurt tulu. Nendeni jõutakse sageli sotsiaalmeedia- ja otsingumootorireklaamide kaudu, samuti telefonitsi. Erakordselt suure potentsiaalse tulu lubadus uinutab ohvri valvsuse. Enamasti kasutatakse pettuseks libaplatvorme ja seal investeerimist õhutavaid libamaaklereid.
- **Armupettus.** Kelm loob kannatanuga usaldusliku suhte, enamasti sotsiaalmeedias, ning hakkab aja jooksul temalt rahalist abi paluma. Sageli tuuakse ettekäändeks vajadus reisida tema juurde, pääseda võlgadest või hankida viisa. Raha võidakse küsida ka ajutise laenuna, mida kunagi tagasi ei maksta.
- **Heategevuspettus.** Ohvriga võtab ühendust näiliselt heategevuslik organisatsioon või isik, kes palub annetada raha. Heategevuse ettekäändel petetakse ohvrit välja raha, sageli pikaajalise manipuleerimise tulemusel.
- **Ettemaksupettus.** Kelm lubab ohvrile suuremat rahasummat, kuid nõuab selle saamise eeltingimusena töötlemistasu, maksu või muu kulu tasumist. Pärast ettemakse tegemist jääb lubatud raha saamata (Nigeeria printsi näide).
- **Maksejuhise muutmine ehk arvepettus (äriühingud).** Ärikliendile saadetakse võltsarve või teade arvelduskonto muutmise kohta, mis suunab maksed kurjategija pangakontole.
- **CEO- ehk juhipettus (äriühingud).** Pettur esineb ettevõtte tippjuhina, kasutades selleks kompromiteeritud meiliaadressi või tehisaru abil loodud võltsvideot või -helisalvestust (deepfake), mida kasutades kästakse raamatupidajal teha kiiresti ja konfidentsiaalselt ülekanne koostööpartnerile, kuid tegelikult jõuab raha petturi kontole.
- **Tööpettus.** Kannatanule pakutakse tööd, kuid palutakse tal enne tasuda tööle asumisega seotud kulud. Tegelikult pole pakutavat töökohta olemas.
- **Turvalise konto pettus.** Ohvriga võetakse ühendust ja väidetakse, et tema raha või väärtpaberid ei ole senises finantsasutuses kaitstud. Vara päästmiseks palutakse tal kanda raha etteantud kontole. Tegelikult kuulub konto kurjategijale, kes raha ei tagasta.

¹ Pettusejuhtumid, mille algatab ja kinnitab ohver omal tahtel, kuigi ta teeb seda sageli manipuleerimise või valeinformatsiooni esitamise tulemusena.

Andmepüük, kontode ülevõtmised ja identiteedivargus²

Kontode ülevõtmiseks (ingl *account takeover*, ATO) kasutatakse mitmesuguseid ründeviise, millest 2025. aastal olid Eestis kõige levinumad mitmeastmelised kõnepettused. Nende käigus võib ohver osa toiminguid ise autoriseerida, näiteks anda manipuleerimise tulemusena petturile ligipääsu oma autentimisvahendile või paigaldada arvutisse kaugjuhtimistarkvara. Erinevalt autoriseeritud maksepettusest kaotab ohver sellisel juhul enamasti kontrolli oma pangakonto üle.

- **Mitmeastmeline kõnepettus ametnikuna või ettevõtte töötajana esinemisega.** Pettus algab tavaliselt näiliselt süütu telefonikõnega. Esimeses etapis võib kelm esineda näiteks kullerfirma töötajana, kes teatab dokumendi saabumisest, või mobiilsideoperaatorina, kes pakub paketi vahetamist või palub andmeid uuendada. Tegelik eesmärk on saada ohvrilt PIN1-koodi abil isikuvastus. Teises etapis helistab ohvrile uus kelm, kes helistab enamasti pangatöötaja või politseinikuna ja hoiatab, et varasema kõne tõttu võib ohvri pangakonto olla ohus. Sageli viiakse vestlus üle teisele suhtlusplatvormile, näiteks WhatsAppi, mida pangad ega politsei kliendiga suhtlemisel ei kasuta. Seejärel võidakse ohvrile väita, et olukorra lahendamiseks korraldatakse politsei salaoperatsioon. Selle käigus palutakse tal kanda raha näiliselt turvalisele kontole ja kinnitada ülekanne PIN2-koodiga.
- **E-posti teel toimuv andmepüük ehk *phishing*.** Ohvrile saadetakse e-kiri, mille saatja aadress ja kujundus sarnanevad panga või teenusepakkuja omadega. Kirjas olev link suunab võltsitud sisselogimislehele, mille kaudu kogutakse kaardiandmeid või muud konfidentsiaalset teavet.
- **Petusõnumid ehk *smishing*.** Saatja andmeid võltsides (*spoofing*) saadetakse ohvrile sõnum, millega meelitatakse teda avaldama oma kaardiandmeid või mobiil-ID/Smart-ID PIN-koode. Näiteks palutakse tal tasuda paki kättetoimetamise eest.
- **Hääländmepüük ehk *vishing*.** See sarnaneb kõnekelmusega: pettur esineb telefonikõnes ametniku või ettevõtte töötajana, et petta ohvrilt välja kaardiandmeid või mobiil-ID/Smart-ID PIN-koode. Hääländmepüük on tõhus, sest petturid saavad samal ajal võita ohvri usalduse ja tekitada temas paanikat, et sundida teda kiirustades tegutsema.
- **QR-koodi pettus ehk *quishing*.** See on uuem pettusevorm, mille puhul kelmid kleeбивad näiteks enda loodud QR-koodi originaalse koodi peale. Koodi skanninud inimene suunatakse võltsitud veebilehele, kus tal palutakse sisestada oma andmed.
- **Reklaamipettus.** Ohvrile kuvatakse internetireklaam või bänner, milles pakutakse näiteks soodsa intressiga kiirlaenu ja palutakse selle saamiseks täita veebivorm. Tegelikult edastab ohver selle kaudu petturitele oma tundlikke isikuandmeid. Selle järgmiseks sammuks on sageli investeerimispettus, mille puhul kasutatakse ära juba ohvri sisestatud andmeid nende ründamiseks.

Kaardipettused³

- **Kaardi vargus või kaotus.** Kaart satub võõrastesse kätte ja seda kasutatakse võimalikult paljude maksete tegemiseks, enne kui omanik või pank jõuab kaardi blokeerida.
- **Card-not-present ehk CNP-pettus.** Varastatud kaardiandmeid kasutatakse internetis või mujal selliste ostude tegemiseks, mille puhul füüsilist pangakaarti ei nõuta.
- **Kaardi kopeerimine ehk skimmimine.** Seda juhtub ennekõike siis, kui ohver sisestab kaardi sularahaautomaati või makseterminali, millele on paigaldatud kaardiandmeid kopeeriv seade. Saadud andmete abil luuakse kloonkaart, mida hakkab kasutama pettur.
- **Point-of-sale ehk POS-pettus.** Makseterminali sisestatakse tegelikust suurem summa,

2 Tegevused, millega pettur omandab ohvri tundlikud andmed, mis võimaldavad petturil tema eest makseid teha.

3 Petturlikud tehingud, mille tegemiseks kasutab pettur pangakaarti, selle andmeid või pangakaardi koopiat.

lootes, et tähelepanematu või joobes ohver maksab näiteks 10 euro asemel 1000 eurot. Samuti võidakse kaardilt võtta sama makse eest raha mitu korda või paigaldada makseterminali skimmimisseade.

- **ATM-pettus ehk sularahaautomaadipettus.** See võib esineda mitmel kujul. Näiteks võib kelm veenda ohvrit võtma sularahaautomaadist raha välja ja andma selle petturile. Kaardiandmetele ligipääsu saanud kelmid võivad aga kasutada füüsilist pangakaarti või digirahakotti, et ohvri kontolt ise raha välja võtta.

NÄITED AKTUAALSETEST PETTUSTEST

Maksejuhise muutmine ehk arvepettus (äriühingud)

- Ettevõtte sai näiliselt oma koostööpartneri nimel saadetud e-kirja, milles paluti ettevõttele edaspidi tasuda arved teisele pangakontole. Tegelikult oli tegemist kelmide loodud libakontoga, kuhu ettevõtte esindaja tegi kahel korral ülekande. Esialgsel andmel on kelmusega tekitatud kahju üle 1,6 miljoni euro.
- Kelmid saatsid ettevõttele e-kirja, milles esinesid advokaadina, kes parajasti abistas ettevõtet välismaale kinnisvara ostmisel. Kirjas teavitati, et kinnisvaratehingu võlausaldajate ehk hüpoteegipidajate pangarekvisiidid on muutunud. Firma kandis raha koostööpartnerite asemel kelmidele kontole. Kelmusega tekitati 1,7 miljoni euro suurune kahju.

Investeeringipettused

- 43aastane naine tutvus Facebookis mehega, kes viis pärast kuuajalist suhtlust jutu krüptorahaga kauplemisele ja investeerimisele. Mees soovitas selleks enda tuttavat maaklerit, kes oleks nõus naist investeerimisel abistama ja juhendama. Septembri alguses sai naine kõne inimeselt, kelle juhendamisel registreeris ta konto kauplemisplatvormil finab.pro ja tegi esimese, 100 dollari suuruse sissemakse. Umbes kolme kuu vältel avas kannatanu väidetava maakleri juhendamisel endale mitu krüptorahakotti ja tegi väidetavalt kauplemisplatvormile ja krüptoadressidele ülekandeid kokku 94 000 euro ulatuses. Selleks võttis naine enda ja tütre nimel mitu laenu ning müüdi ka tütrele kuuluv korter. Samuti andis naine mitmel korral sularaha kulleritele, arvates, et investeerib selle platvormile. Kannatanu ei saa platvormil kuvavat raha välja võtta ning temalt nõutakse lisamakseid. Esialgsel hinnangul tekitati kelmusega 122 000 eurot kahju.
- Anija vallas elav mees luges internetist libaartiklit, milles näiliselt Margus Linnamäe rääkis investeerimisest ning jättis veebilehele enda kontaktandmed. Hiljem võttis mehega telefoni teel ühendust inimene, kelle juhendamisel avas ta endale krüptorahakoti ja kontod Revolutis, Bigbankis ja Mercuryos ning tegi platvormile esimese sissemakse. Järgmise paari kuu jooksul võimaldas kannatanu kelmide juhendamisel Anydesk programmi kaudu kaugjuurdepääsu oma seadmele, võttis laenu ning tegi ülekandeid enda nimele avatud krüptorahakotti. Kannatanu ei saa platvormil kuvavat teenitud raha välja võtta. Esialgsel hinnangul tekitati kelmusega 36 529 eurot kahju.

Mitmeastmelised kõnepettused

- Kannatanule helistati ja küsiti, kas tema ja ta abikaasa saavad ravimitelt soodustust. Kannatanu vastas eitavalt, mille peale teatas helistaja, et ta võib vormistada kaardi, mille alusel saavad nad edaspidi apteegist ravimeid soodustusega osta. Seejärel ütles helistaja, et kannatanu ja tema abikaasa peavad minema polikliinikusse analüüsi andma ja tervises seisundit kontrollima. Lisaks küsis helistaja nende perearsti nime ja kodust aadressi, mille kannatanu ka avaldas. Seejärel helistas kannatanule teine kelm, kes esitles end politseinikuna ning väitis, et eelnev kõne oli pettus. Ta lubas, et hakkab neid nüüd juhendama, kuidas nende raha petturite käest päästa. Kelm ütles, et nad ei tohi toimuvast kellelegi rääkida, sest selle eest on ette nähtud karistus, ning leppis kokku salasõna. Kannatanu pidi panema enda ja abikaasa pangakaardid ümbrikusse ning andma selle kullerile, kes ütleb õige salasõna. Kelm lisas, et kuller kannab viiruse leviku tõkestamiseks maski. Umbes pool

tundi hiljem tuligi vanapaari koju maskis mees, kellele nad andsid pangakaarte sisaldava ümbriku. Veidi hiljem helistas kelm uuesti ja kinnitas, et sai ümbriku kätte ning toonitas, et nad mitte mingil juhul kellelegi sellest ei räägiks. Hiljem tekkis kannatanul kahtlus. Ta proovis väidetavale politseinikule tagasi helistada, kuid number ei olnud kättesaadav. Seejärel pöördus kannatanu politseisse.

- Kannatanule helistati esmalt veearvesti vahetamise ettekäändel. Seejärel sai mees kõne väidetavalt politseikomissarilt, kes ütles, et petturid on sihikule võtnud tema korteri ja oleksid selle temalt ära võtnud, kui politsei poleks sekkunud. Mehele öeldi, et ta peab nüüd uurimisasutustega koostööd tegema, et aidata petturid tuvastada ja kinni pidada. Selleks käskis kelm mehel helistada tema antud telefoninumbri kinnisvara ostvale firmale ja teeselda söödana tegutsedes, et soovib oma korterit müüa. Kelm kinnitas, et kui mees aitab riiki, aitab riik teda. Samuti rõhutati, et mees ei tohi uurimisest kellelegi rääkida, viidates väidetavale konfidentsiaalsuse paragrahvile. Seejärel pidi mees sõlmima korteri fiktiivse müügilepingu ning korteri ja sellega seotud dokumendid ümber vormistama. Lisaks anti talle väga selged juhised notariga rääkimiseks, et mitte kahtlust äratada. Kui korteri müügist saadud raha oli mehe kontole laekunud, kästi tal see väidetavasse kindlustusfondi kanda ning registreeruda krüptobörsil. Kuna kannatanu pank keeldus ülekandeid tegemast, käskisid kelmid tal raha kanda teise pank, võtta osa sellest välja sularahas ja ülejäänu eest osta kullakange. Kelmid lubasid, et niipea kui raha on välja võetud, vormistatakse korter mehe nimele tagasi. Korterimüügist saadud raha ja selle eest ostetud kullakangid andis mees kelmide saadetud rahakulleritele.

Kulleriskeemid

- Kannatanu sai näiliselt Omniva kullerilt kõne, milles öeldi, et talle on saabunud tähtis kiri. Kirja kättesaamiseks saatis helistaja naise seadmesse Smart-ID kinnituskoodi ning naine kinnitas kelmide algatatud toimingut oma PIN-koodiga. Mõned minutid hiljem sai naine uue kõne, seekord väidetavalt politseist. Naisele väideti, et tema kontol on toimunud kahtlane sisselogimine ja tõenäoliselt on tegu kelmidega. End politseinikuna esitlenud kelm ütles, et kohe võtab naisega ühendust ka panga esindaja, kes selgitab, mida ta peab oma raha päästmiseks tegema. Kelmid käskisid naisel viia pangakaardid juurduse huvides pakiautomaati ega lubanud tal toimuvast kellelegi rääkida, kuna see võivat uurimist takistada. Lisaks väitsid kelmid, et naise sõiduauto peale tahetakse laenu võtta ning soovitasid panna sõiduki müüki, et kelmid ei saaks seda kasutada. Nad juhendasid naist, kus autot müüa, ja väitsid, et sõiduki ostja on rahapesuga tegelev kelm, kelle nad pärast tehingut vahele võtavad. Auto müügist saadud raha pidi kannatanu samuti uurimise huvides pakiautomaati viima. Kelmid lubasid, et kui kõik tõendid on kogutud, saab naine järgmisel päeval auto tagasi. Naine ei saanud tagasi ei autot ega raha ning kaotas kelmidele üle 21 000 euro.
- Ettevõtjale helistas eesti keelt kõnelev kelm, kes esitles end Omniva kullerina. Kelm teatas mehele, et talle on saabunud Tartu maakohust tähtis kiri. Kuna kannatanu oli hiljuti täitnud dokumente ja ajanud ettevõttega seotud asju, tundus kõne talle usutav. Lisaks oli kannatanu parajasti tööga hõivatud, mistõttu polnud tal aega pikalt järele mõelda. Väidetav kuller lubas panna kirja pakiautomaati ja edastada mehele telefonitsi selle kättesaamiseks vajaliku koodi. Kõne ajal tuli mehe telefonile Smart-ID autentimistaotlus, milles ta valis kuvatud kinnituskoodi. Seejärel tuli ette PIN1-koodi sisestamise koht. Kelm oli samal ajal vait ega survestanud meest, vaid kannatanu sisestas koodi Smart-ID rakendusse ise. Paar minutit peale esimese kõne lõppu sai mees uue kõne eesti keelt kõnelevalt mehelt, kes väitis end olevat politseinik Heiki Reest. Politseinikuna esinenud kelm ütles, et kannatanu andmed on kelmide käes, kes võtavad juba tema nimele laene, ning nüüd on vaja pangakontosid kiiresti kaitsma hakata. Edasi selgitas helistaja kannatanule pikalt, kuidas kelmid tegutsesid, et usaldust äratada. Seejärel suunati kõne järgmisele kelmile, kes esitles end SEB töötaja Maksim Reimanina. Kannatanu järgis helistajate juhiseid, mille tulemusel logiti tema internetipanka ning hakati väidetavalt raha kaitsmiseks tema ja talle kuulunud ettevõtete kontodelt tegema ülekandeid võõrastele pangakontodele.

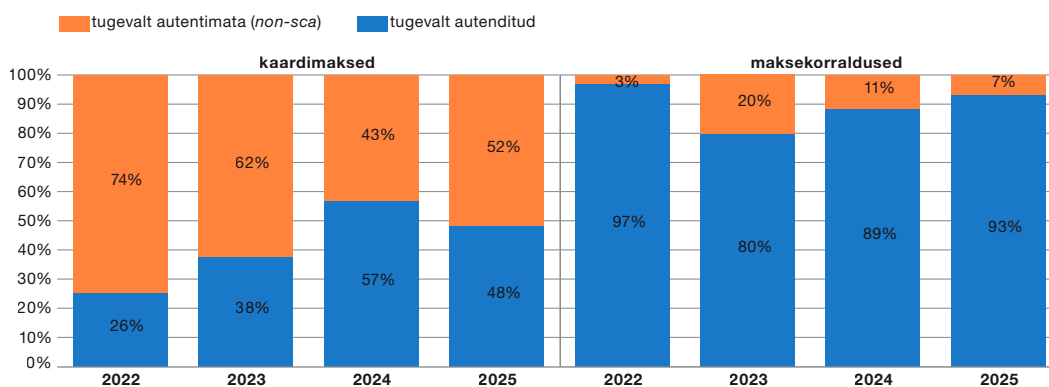
PETTUSTE ALGATAMISE VIISID

Maksekorralduspettused

Eesti Panga kogutud statistika põhjal oli 93% viimase aasta jooksul tehtud maksekorralduspettuse tehingutest tugevalt autenditud (vt joonis 1). Interneti- või mobiilipangas tehtud maksekorralduste puhul rakendatakse tugevat autentimist, kui tehing kinnitatakse lisaks keskkonda sisselogimisele Smart-ID, Mobiil-ID, ID-kaardi, PIN-kalkulaatori või muu kahefaktorilise autentimismeetodiga, tihti PIN2-koodi sisestades. Taoliste maksekorralduspettuste hulka kuuluvad autoriseeritud maksete pettused (*authorised push payment*, APP), aga ka mitmesugused andmepüügi- ja identiteedivarguse skeemid.

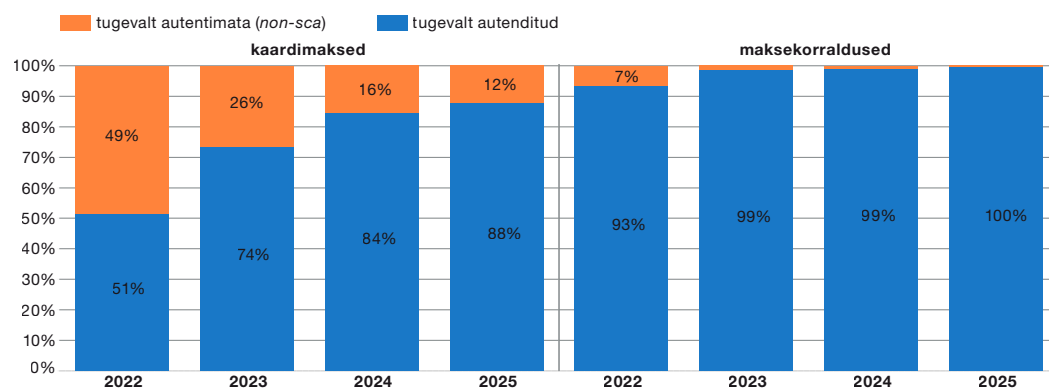
APP-pettuse puhul meelitatakse ohvrit kandma raha enda kontolt kelmi kontrolli all olevale kontole. Tavapärastest pettuste ennetamise meetmetest, mis on suunatud konto ligipääsu kontrollidele, ei pruugi selliste maksekorralduspettuste puhul abi olla, sest ohver on ise makse algatanud ja kinnitanud. Enim mõjusad ennetusmeetmed on elanikkonna informeerimine ja teadlikkuse tõstmine.

Joonis 1. Autentimise tugevus tehingute arvu osakaalu järgi



Allikas: Eesti Pank.

Joonis 2. Autentimise tugevus käibe osakaalu järgi



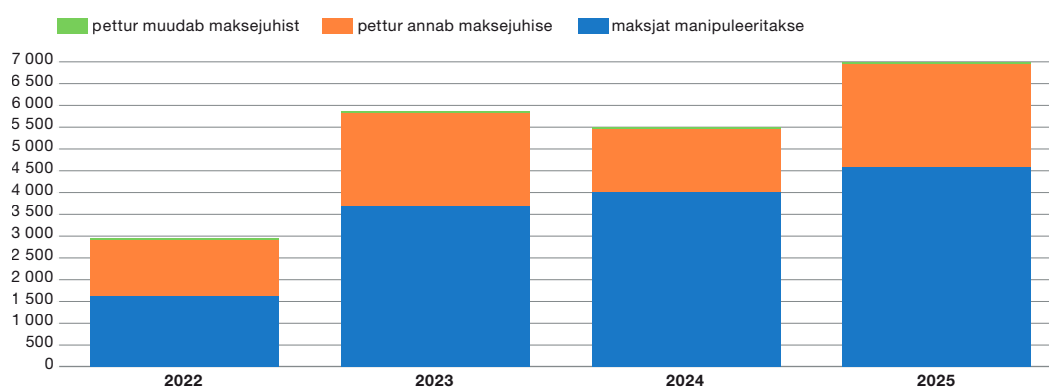
Allikas: Eesti Pank.

Autoriseeritud maksekorralduspettuste hulka kuuluvad näiteks investeerimispettused ja nn turvalise konto pettused, mitmeastmelised kõnekelmused, mille puhul meelitatakse ohvrit raha „turvalisse kohta“ kandma, ning ettemaksupettused lubadusega hiljem rohkem raha tagasi maksta. Autoriseeritud maksekorralduspettustega tekitatud kahjust pärineb ligi 100% tugevalt autenditud tehingutest (vt joonis 2). Muud autentimata tehingud on peamiselt väikemaksed, mis ei vaja PIN2 kinnitust, või kordumaksed. Maksekorralduspettused tuginevad üldiselt näilisele hädavajadusele teha tehing kiiresti või lubadusele teenida lühikese ajaga suurt kasumit. Seetõttu teevad ohvrid kahel kolmandikul juhtudest ülekandeid

kelmidele ise olukorras, kus kiirustamise tõttu on nende tähelepanu makse sisult kõrvale juhitud (vt joonised 3 ja 4). Teine petturite kasutatav võte on saada juurdepääs ohvri kontole ja anda maksejuhise tema asemel. Seda juhtub kolmandikul juhtudest. Sellise etapiviisilise pettuse korral püütakse esmalt saada inimeselt kätte tema turvakoodid. Nende abil saab pettur ise internetipanka sisse logida, konto seadeid muuta, sealhulgas makselimiite suurendada, ohvri nimel kiirlaenu taotleda ja makseid algatada, et raha kiiresti rahamuulade kontodele kanda.

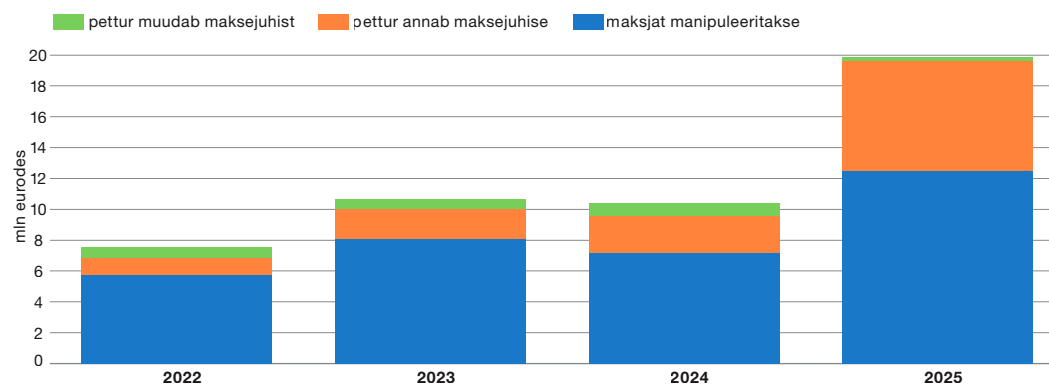
Rahamuul on inimene, kes liigutab ebaseaduslikult saadud raha mitme maksekonto vahel ja saab selle eest vahendustasu. Tema eesmärk on varjata pettuse või muu kuritegeliku tegevusega saadud raha päritolu ja aidata raha kiiresti edasi kanda. Rahamuulade kasutatavad maksekontod asuvad sageli eri riikides.

Joonis 3. Maksekorralduspettuste tehingud algatamise järgi



Allikas: Eesti Pank.

Joonis 4. Maksekorralduspettuste käive algatamise järgi



Allikas: Eesti Pank.

Petturid panevad suurt rõhku sellele, et suhtlus ohvriga kestaks võimalikult kaua, et tal ei tekiks võimalust helistada panka, pereliikmele või mujale abi saamiseks. Suhtlus ei lõpe alati pettuse toimepanekuga, vaid võib jätkuda veel mitu tundi, et petturitel oleks aega raha edasi kanda, näiteks rahamuulade kontodele. Sellega maandavad kelmid riski, et ohver liiga kiiresti pettusest või selle kahtlusest kellelegi teada annab. Pika suhtluse teine eesmärk on hajutada ohvri tähelepanu, et ta ei märkaks kahtlaseid detaile, nagu veebilehe võltsitud aadress, tavapärasest erinev autentimiskeskkond või ebatavaliselt sage PIN1- ja PIN2-koodi sisestamine. Sellistes olukordades aitab kõige paremini rahunemispaus, isegi kui tegemist näib olevat hädaolukorraga. Enne ülekande tegemist tuleks alati läbi mõelda, millest tehingu algatamine alguse sai. Kui ajendiks oli teise poole algatatud kõne, on pettuse oht suur, eriti juhul, kui vestlus viiakse üle suhtlusrakendusse, näiteks WhatsAppi või Telegrami. Ohvreid manipuleeritakse

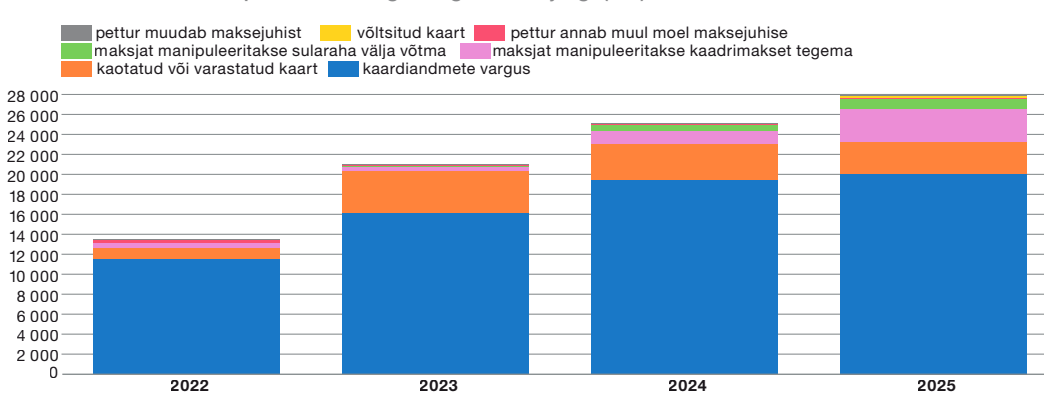
uskumaks, et suhtlusplatvormide kaudu ühendust võtnud libapolitsei või muud -ametnikud on kaasanud isikuid osalemaks „salaoperatsioonis“, mistõttu on nad väga pikalt petturite mõju all, sest usuvad end aitavat enda ja teiste ohvrite raha päästa. Äärmiselt ohtlikud on olukorrad, kus väidetavat probleemi saab lahendada üksnes raha teisele kontole kandes või kus helistaja palub avaldada PIN-koode või kinnitada tema suunamisel autentimispäringuid.

Kaardipettused

Kaardipettused jagunevad maksetehingu algatamise viisi järgi kaheks: füüsilise kaardiga tehtud tehinguteks ja kaugtehinguteks, mille puhul kasutatakse üksnes pangakaardi andmeid (*card not present*). Esimesel juhul võidakse võltsitud või varastatud pangakaardiga sularaha välja võtta või sellega makseterminalis maksta. Teisel juhul on kurjategijad kaardiandmed enda valdusse saanud ja kasutavad neid veebitehingute, seal hulgas internetiostude tegemiseks. Kaarditehingute pettustest on 48% autenditud kaardipettused (vt joonis 1). See tähendab, et ülejäänud 52% pettuslikest tehingutest kuuluvad kas Euroopas kehtivate tugeva autentimise nõuete erandite alla või tehti näiteks väljaspool Euroopat tegutsevate kaupmeeste juures, kes pole kohustatud rakendama 3D Secure'i meetmeid. 3D Secure suurendab internetipoes tehtavate kaarditehingute turvalisust, suunates kaardiomaniku iga ostuga kõigepealt oma isikut tuvastama panka sisse logides või muu tuvastusvahendi kaudu, näiteks Smart-IDga. Autentimata kaarditehingute puhul võib piisata kaardiandmete sisestamisest internetipoes. Autentimata tehingute hulka kuuluvad ka näiteks väikese summaga NFC- ehk viipemaksed. Teisalt aga moodustavad autentimata tehingud ainult 12% kaardipettustega tekitatud kahjust. See tähendab, et isegi kui neid on rohkem kui pool kaardipettustest, liigituvad nad peamiselt kahjude mõistes pisipettusteks (vt joonised 1 ja 2).

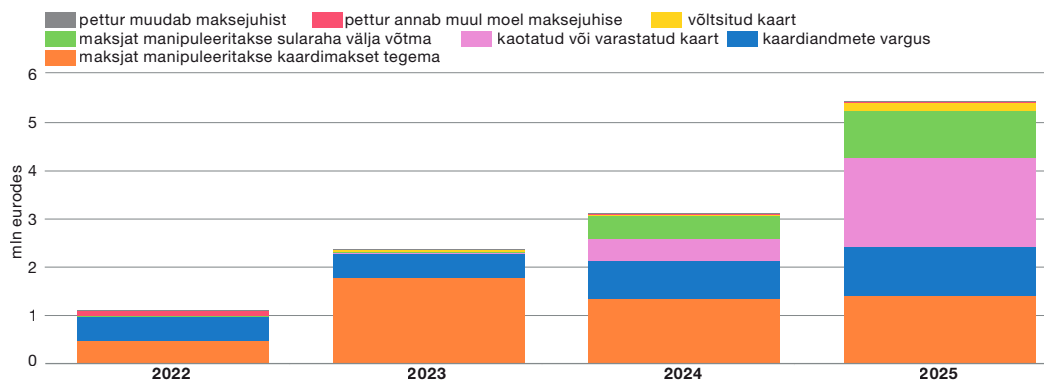
Alates 2020. aastast, kui Euroopas kehtestati tugeva autentimise nõue, on petturid pidanud leidma uusi petuskeeme, sest tugevalt autentimata tehingute ärakasutamise võimalused vähenesid märgatavalt. Nii joonistub eriti kaarditehingute puhul välja, kuidas viimaste aastate jooksul on tugevalt autenditud kaardipettuste osakaal järsult kasvanud: 26%-lt 48%-le (vt joonis 1). See näitab, et pettuste tõkestamise meetmed on paranenud, kuid petturid kasutavad üha rohkem ohvrite manipuleerimist ja pettuste hulk kasvab sellele vaatamata. Kaardipettusi on palju, kõige rohkem esineb nende seas e-kaubandusega seotud pettusi. Selleks, et tugevast autentimisest mööda pääseda, on kelmid hakanud viimastel aastatel rohkem kasutama varastatud kaardiandmeid (vt joonised 5 ja 6). Peamiselt tehakse varastatud andmetega e-kaubanduse kaarditehinguid väljaspool Euroopat ja kõige populaarsemaks kohaks on osutunud Ameerika Ühendriikide internetipoeid. Internetist ostes tasub olla ettevaatlik ja uurida enne ostu sooritamist internetipoe või müüja tausta. Eriti tasub seda teha siis, kui ostjale pakutakse ebaharilikult suuri soodustusi.

Joonis 5. Kaardimaksepettuste tehingud algatamise järgi (arv)



Allikas: Eesti Pank.

Joonis 6. Kaardimaksepettuste käive algatamise järgi



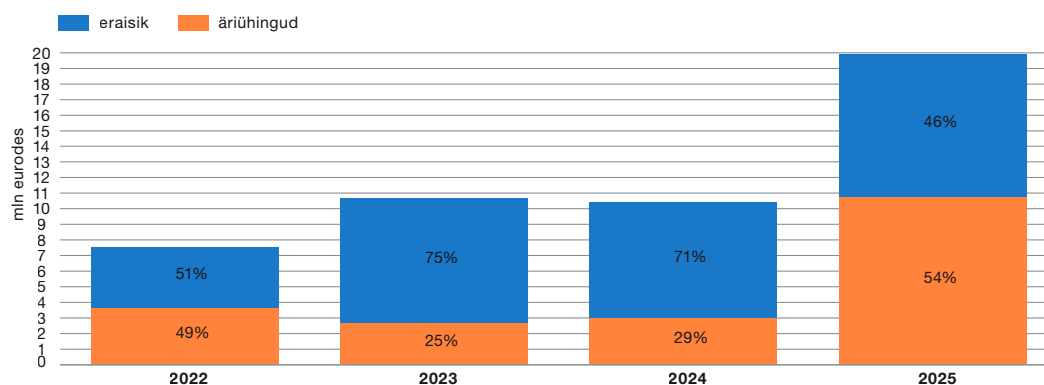
Allikas: Eesti Pank.

Internetist ostes tuleb seega olla väga ettevaatlik ja veenduda ostukoha turvalisuses. E-poe turvalisuse hindamisel tasub näiteks kontrollida, kas sellel on Eesti E-kaubanduse Liidu väljastatud usaldusmärgis „Turvaline ostukoht“. Samuti tasub e-poe kohta teha taustakontrolli, otsida arvustusi ja pöörata tähelepanu sellele, kui värsked on positiivsed hinnangud. Üle tuleks kontrollida ka see, kas veebilehel on avaldatud ostu-, tarne- ja tagastamistingimused ning kontaktandmed. Kui kaup või teenus jääb kätte saamata, peab tarbija kõigepealt pöörduma kaupmehe poole. Tehingu vaidlustamisel tuleb tõendada, et kaupmees pole nõustunud kaupa saatma ega raha tagastama. Võimaluse korral tasub kasutada madala limiidiga virtuaalkaarti või virtuaalse kaardinumbri teenust, mille kasutamisest saab hõlpsalt loobuda. Kaardiandmete lekkimise korral saab virtuaalkaardi sulgeda ning võimalikku kahju piirata. Veel üks levinud füüsilise kaardiga seotud pettus on kaardi kopeerimine ehk skimmimine, mille tõkestamiseks on pangad võtnud kasutusele sularahaautomaate ja pangakaarte kaitsvad meetmed. Tänapäeval kohtab skimmimist Euroopas harva, kuid väljaspool Euroopat võib kaardiandmeid kopeerivaid seadmeid siiski ikka veel makseterminalidelt leida.

Ettevõtetega seotud pettused

Viimastel aastatel on üha enam sattunud petturite sihtmärgiks ettevõtted ja seda põhjusel, et saada ligipääs nii eraisiku kui ka ettevõtte kontole. Nii on petturil võimalik korraga rohkem raha välja petta. Seda näitab ka kahju kasv, mis on olnud pettuste arvu kasvust kordades kiirem. Ettevõtetega seotud pettused moodustavad ainult 15% kõigist petturlikest tehingutest, eraisikutega seotud juhtumid aga 85%. Samas näitab 2025. aasta kohta tehtud statistika, et äriühingute osa pettustega tekitatud kogukahjust kasvas võrreldes eraisikutega 29%-lt 54%-ni. Seega langes üle poole kahjust ettevõtete kanda (vt joonis 7). Kõige suuremad ühekordsed kahjud tekivad maksejuhise muutmise ehk arvepettuse tõttu. Selle skeemi puhul saavad petturid juurdepääsu koostööpartnerite meilikontole. Kuna ettevõtted teevad sageli

Joonis 7. Eraisikute ja äriühingute maksekorralduste kahjude jaotus



Allikas: Eesti Pank.

rutiinseid makseid, kujuneb partnerite vahel usaldus ning koostööpartneri meilikontolt saadetud teade pangarekvisiitide muutmise kohta ei pruugi kohe raamatupidajale kahtlane tunduda. Nii on viimastel aastatel selliste üksikjuhtumite suurim kahju ulatunud 1,7 miljoni euroni. Usaldus koostööpartneri vastu on suur, aga veel keerulisem on olla skeptiline oma firma juhilt tulnud korralduse suhtes. Üldiselt võetakse juhipettuse puhul sihikule maksete tegemise õigusega töötaja, keda meelitatakse tegema autoriseerimata ülekandeid. Lihtsama skeemi korral saadetakse töötajale juhi nimel võltsitud e-kiri. Keerulisemates olukordades võidakse kasutada *deepfake*'i ehk süvavõltsingut koos veebikohtumisega. Seetõttu pakuvad selliste pettuste vastu parimat kaitset selged organisatsioonisisemed kontrollimeetmed ja kokkulepitud finantshügieeni põhimõtted. Kui sätestada, et teatavat piirmäära ületavate tehingute puhul rakendatakse alati nelja silma põhimõtet ja olulisi muudatusi kontrollitakse teise kanali kaudu, saab enamikku suurtest kahjudest ennetada. Näiteks tuleks suure koostööpartneri teatatud pangakonto muutus kinnitada temaga varem kokku lepitud kontaktandmetel.

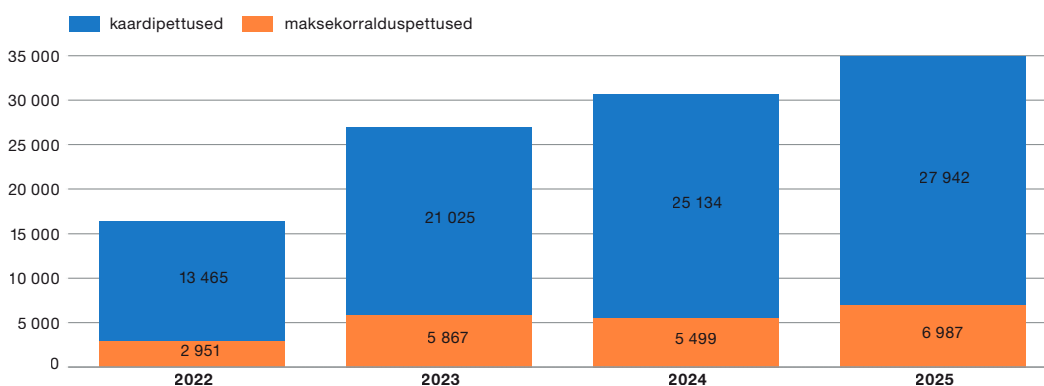
Ettevaatlikud ei pea olema mitte ainult ettevõtted, vaid ka korteriühistu juhatuse liikmed, kellel on lisaks enda erakontole ligipääs ka korteriühistu rahadele. Olukorra teeb keeruliseks see, et petturid otsivad avalikest andmebaasidest korteriühistutega seotud inimesi ja kasutavad nende puhul ka tavapäraseid petuskeeme, nagu kulleri kõnekelmus, et korteriühistule näiliselt saabunud tähtis kirja kinnitada. Nii loodavad petturid kätte saada korteriühistu kinnitatud PIN1-koodi pangakontole ligipääsemiseks ja seeläbi muu ametnikuna esinedes erinevatel ettekäändel PIN2-koodi kätte saada. Tihti on korteriühistute kontodel suured summad, mis on kogunenud remondifondi sissemaksetest ja muudest tasudest, samas aga võivad puududa tavapäraseid kaitsemeetmed, näiteks nelja silma printsiip ülekannete tegemisel. Seetõttu on rünnakud suunatud just eraisikutele läbi mitmeastmeliste kõnekelmuste, kellel on samas ligipääs juriidiliste isikute kontodele, seal hulgas raamatupidajad ja juhatuse liikmed. Sama probleem puudutab ka väikeettevõtjaid ning kelmid teavad väga hästi, kuidas selliseid turvanõrkusi ära kasutada. Seetõttu tuleb nii ettevõtetes kui ka korteriühistutes hoolikalt üle vaadata, milliseid turvameetmeid rakendatakse ja kuidas ennast kelmide võimalike petuskeemide eest paremini kaitsta. Suuremate või ebatavaliste maksete kinnitamiseks tuleks võimalusel nõuda vähemalt kahe inimese heakskiitu ning piirata kasutajate õigusi ja ülekandelimiite vastavalt tegelikule vajadusele. Samuti tuleks makse saaja kontoandmete muutmine alati üle kontrollida varem teada olnud kontaktkanali kaudu. Kinnitada ei tohiks Smart-ID või Mobiil-ID päringuid, mille algatamise põhjus ei ole täielikult selge.

PETTUSTE STATISTIKA

Pettuste käive ja tehingute arv

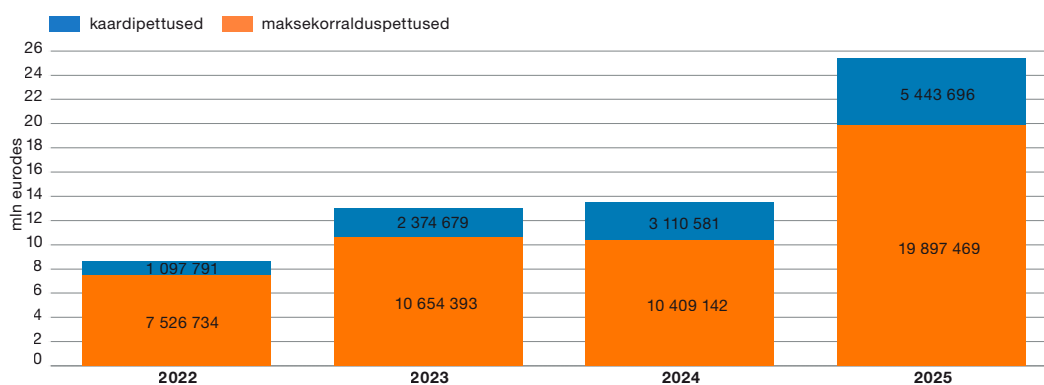
Eesti Panga andmetel on viimase nelja aasta jooksul nii maksekorraldus- kui ka kaardipettuste arv stabiilselt kasvanud, kuid veelgi muret tekitavam on kahjude plahvatuslik suurenemine just 2025. aastal. Eesti pangakaartidega tehti mullu 28 000 kaardipettust, mida on 11% rohkem kui 2024. aastal. Kaardipettuste tagajärjel kaotasid inimesed petturitele 5,4 miljonit eurot, mis märgib 75% kasvu võrreldes eelneva aastaga (vt joonised 8 ja 9). Maksekorralduspettuste arv kasvas 2025. aastal 7000 tehinguni ehk 27% võrreldes eelmise aastaga. Nende pettuste käive suurenes kogunisti 91%, ulatudes 19,9 miljonit euron. Kokku kasvas pettuste käive 2025. aastal pankade edastatud andmetel 25,3 miljoni euroni ja pettuste arv 34 900 tehinguni. Aasta varem olid vastavad näitajad 13,5 miljonit eurot ja 30 600 tehingut. Seega suurenes pettustega tekitatud kahju ligi kaks korda.

Joonis 8. Pettuste arv



Allikas: Eesti Pank.

Joonis 9. Pettuste käive



Allikas: Eesti Pank.

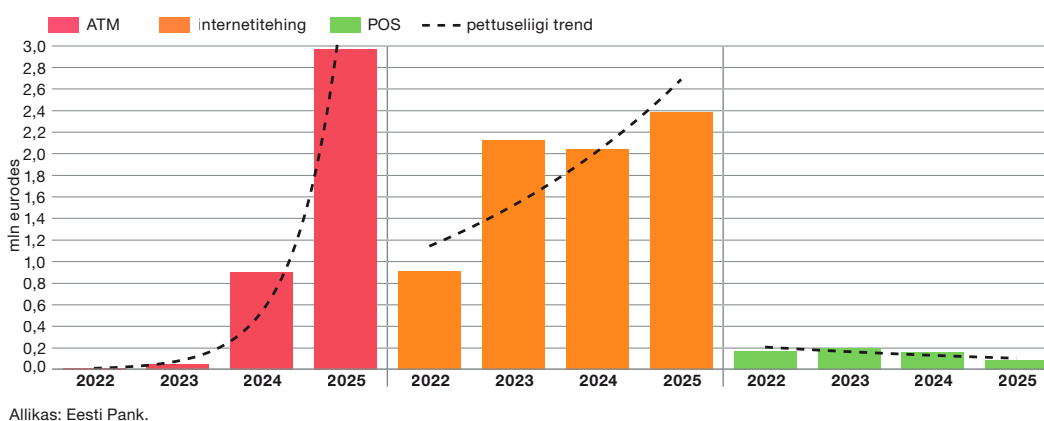
Tavapäraseid kaarditehinguid tehti 2025. aastal 526,2 miljonit koguväärtusega 14,8 miljardit eurot. Maksekorraldustehinguid tehti samal ajal 292,3 miljonit ja nende koguväärtus ületas 383 miljardit eurot. Iga tuhande elaniku kohta langes kaardipettuse ohvriks 20 inimest ehk kaks inimest rohkem kui aasta varem. Maksekorralduspettuse ohvriks sattus 2025. aastal viis inimest tuhande kohta, mida on üks rohkem kui 2024. aastal.

Pettuste liigid

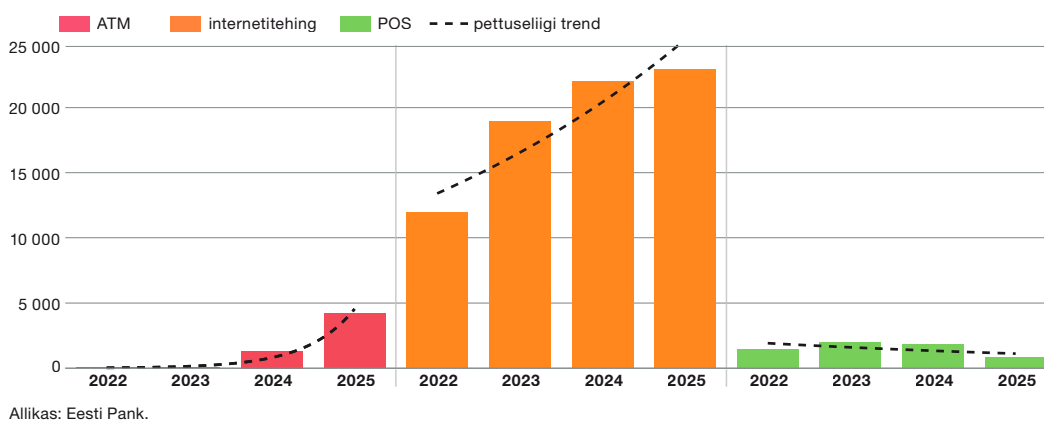
Eesti pangakaartidega 2025. aastal toime pandud pettuste arvust moodustasid 55% sularahaautomaadi- ehk ATM-pettused (3 miljoni euro väärtuses), 43% internetipettused (2,4 miljoni euro väärtuses)

ja 2% makseterminali- ehk POS-pettused (86 000 euro väärtuses) (vt joonis10). Märkimisväärne on ATM-pettustega tekitatud kahjude kasv: see enam kui kolmekordistus 2025. aastal, ületades e-kaubanduse ehk internetipettustega tekitatud kahju. ATM-pettused jagunevad kolmeks: kaotatud või varastatud kaardi kasutamine, maksja manipuleerimine sularaha väljavõtmiseks ja võltsitud kaardi kasutamine (vt joonised 5 ja 6). 61% ehk 1,8 miljonit eurot kahjusid tuleb kaotatud või varastatud kaardi pettustest, mis on üldjuhul seotud füüsilise kaardi ja PIN-koodi väljapetmise või rahakulleriskeemidega. Sellisel juhul annab ohver pangakaardi koos PIN-koodidega tavaliselt ümbrikus rahakullerile või jätab selle petturi juhiste järgi pakiautomaati. Maksja manipuleerimisega sularaha väljavõtmiseks tekitatud kahju moodustas 33% ATM-pettuste kahjust ehk 960 000 eurot. Selliste pettuste puhul manipuleeritakse ohvrit ise sularaha välja võtma ja seda petturitele üle andma. Oluline on märkida, et kuigi ATM-pettustest on saanud tekitatud kahju poolest suurim kaardipettuste liik, tehakse neid tehinguid võrreldes internetipettustega pea viis korda vähem. See näitab, et ühe ATM-pettuse kohta tekitatud kahju on väga suur (vt joonis 11).

Joonis 10. Kaardimaksepettuste käive tehinguliigi järgi



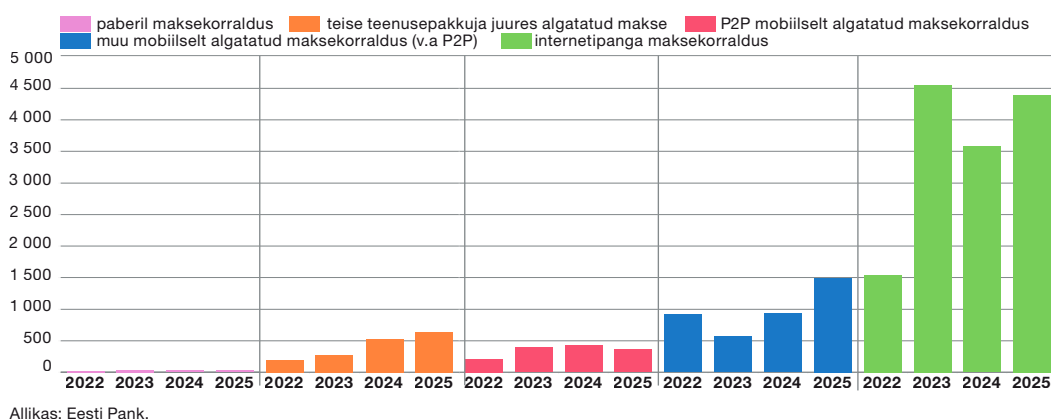
Joonis 11. Kaardimaksepettused tehinguliigi järgi (arv)



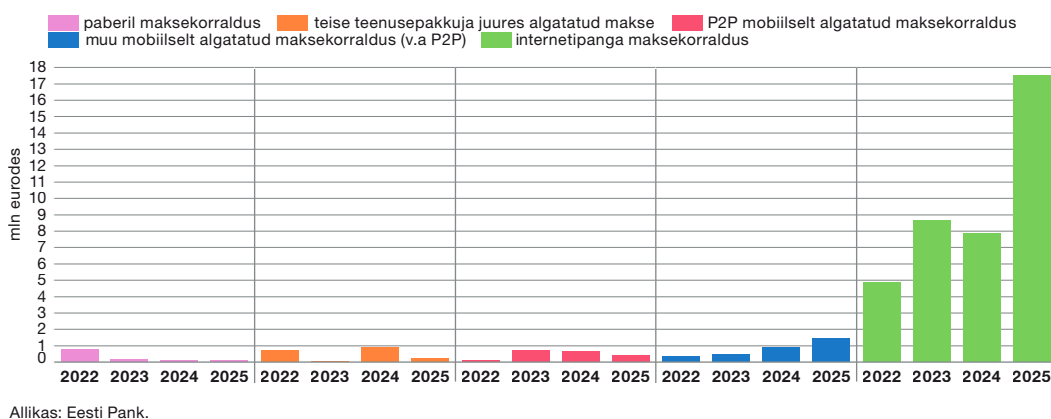
Läbi aastate on pangakaartidega seotud internetipettused olnud peamine kahju põhjustav pettuseliik. Nende kaks peamist vormi on maksja manipuleerimine kaardimakse tegemiseks ja kaardiandmete vargus. 2025. aastal moodustasid need internetipettuste kogukahjustest vastavalt 1,36 miljonit eurot ehk 57% ja 1 miljon eurot ehk 42%, kokku 2.4 miljonit eurot (vt joonis 10). Kaardimakse tegemise manipuleerimise alla lähevad erinevad skeemid, et meelitada inimest ostma libakaupmeeste internetipoodidest suurte allahindlustega, ja ostupettused, mille puhul toode kunagi kohale ei jõua. Kaardiandmete varguse puhul on inimese kaardiandmed lekkinud või varastatud ning keel kasutab neid hiljem tehingute tegemiseks. Taolisi pettusi tehti 2025. aastal peaaegu 23 000 (vt joonis 11).

Maksekorralduspettuste puhul on 89% pettustest internetipangas tehtud maksekorraldused, mis moodustasid 2025. aastal 17,5 miljonit eurot maksekorralduspettuste käibest (vt joonised 12 ja 13). Muude mobiilselt algatatud maksekorralduste (v.a P2P) osakaal oli 7% ehk 1,4 miljonit eurot. Ülejäänud 4% moodustasid P2P-mobiilimaksed, paberil esitatud maksekorraldused ja teise teenusepakkuja juures algatatud maksed. Nii tehingute arvu kui ka käibe poolest on levinuim ohvri manipuleerimine maksekorraldust tegema ehk pettus, mille puhul ohver kannab ise petturitele raha üle (vt joonised 3 ja 4).

Joonis 12. Maksekorralduspettused tehinguliigi järgi (arv)



Joonis 13. Maksekorralduspettuste käive tehinguliigi järgi

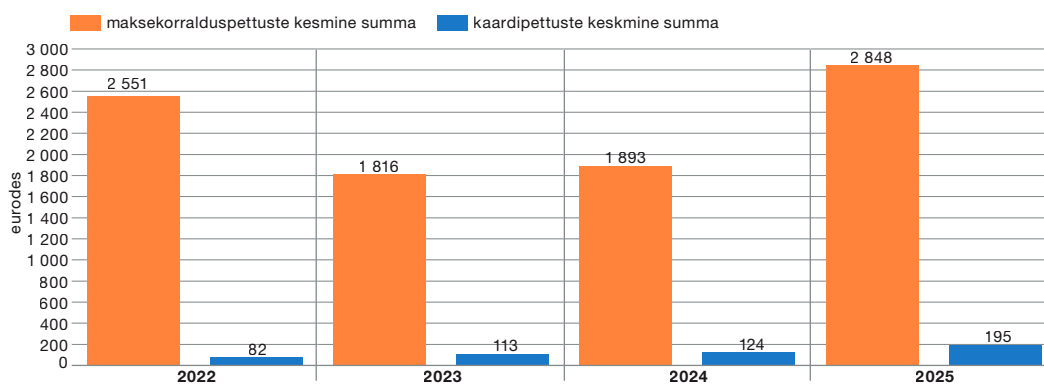


Pettuste liike on palju ja kelmid püüavad tihti ohvritele läheneda eri kanalite kaudu: meilide ja vestlusrakenduste vahendusel, sotsiaalmeedias, arvutiviiruste abil, järelturul kaupu ostes või müües ning ka lihtsalt füüsiliselt, näiteks rahakullereid kasutades. Olenevalt petuskeemist kasutatakse ka spetsiaalset tarkvara, mis on kohandatud nõnda, et need kuvaksid ohvri telefonis võltsitud pangalehte või muud sisselogimiskeskkonda. Tuleb ka arvestada, et suurte keeltemudelite (LLM) arengu ja levikuga muutub organiseeritud kuritegevusel aina lihtsamaks luua ajutisi veebilehti, mis jäljendavad pankade ja teiste asutuste, näiteks telekommunikatsiooniettevõtete veebilehti. Kui telefonikõnega lõksu meelitatud ohver sisestab oma PIN-koodi keskkonda, mis näeb välja nagu tema kodupank, näeb kelm koodi reaajas ja saab kuvada ohvri telefonis uue vaate, et lisainfot küsida. Endiselt tuleb olla eriti ettevaatlik just välismaistes e-poodides, et vältida nii libakaupmeeste võltsveebilehtedelt ostmist kui ka raha kandmist tundmatutele isikutele või firmadele. Kelmid kasutavad inimeste teadmatust osavalt ära, rakendades psühholoogilist survet, veenvat jäljendamist ja andmepüüki, et panna ohvreid tehinguid tegema või tundlikke andmeid avaldama. Üldiselt moodustab kokkupuude ohvriga siiski vaid väikese osa kogu pettuseahelast. Sellele eelneb sageli põhjalik ettevalmistus ning ka pärast pettuse toimepanemist tuleb kurjategijatel saadud raha rahamuulade kaudu raha edasi liigutada.

Pettuste keskmised kahjusummad

2025. aastal oli keskmine kaardipettuse kahjusumma 195 eurot ja 2024. aastal 124 eurot. Maksekorralduspettuse keskmine suurus kasvas samuti: 1893 eurot 2024. aastal 2848 eurole 2025. aastal (vt joonis 14). Maksekorralduspettuse keskmise kahjusumma arvutamisel on arvesse võetud nii eraisikuid, ettevõtteid kui ka muid ühinguid ja fonde. Ainult eraisikuid arvestades oleks keskmine kahjusumma 1570 eurot. Väärib märkimist, et eraisikute tavapärase maksekorralduse keskmine summa on 160 eurot. Maksekorralduspettuste summa on seega ligikaudu kümme korda suurem kui tavapärane maksekorraldustehing. Seda erinevust selgitavad muu hulgas investimispettused, mille puhul liiguvad sageli suuremad summad. Tavapärase kaarditehingu keskmine summa on 28 eurot, samal ajal kui kaardipettuse keskmine kahjusumma on ligi seitse korda suurem. Kaardipettuste keskmist kahjusummat mõjutavad suuremate summadega e-ostu- ja sularaha väljavõtmise pettused.

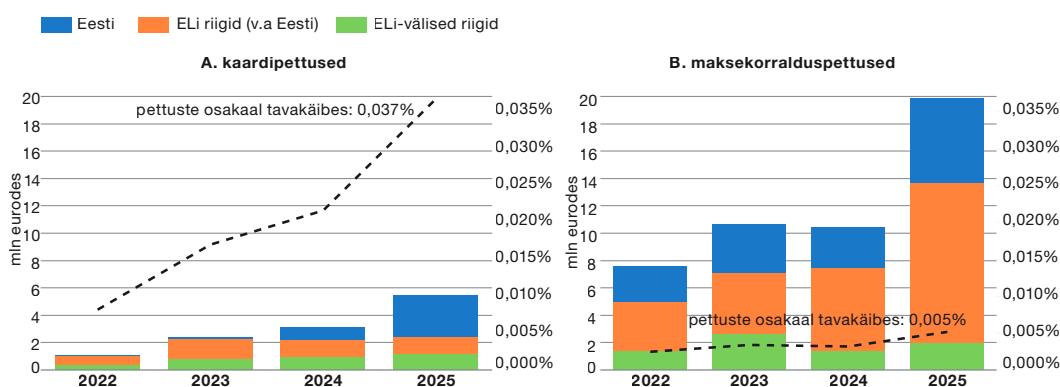
Joonis 14. Kaardimaksete ja maksekorralduste keskmine pettuste ja tehingute summa



Allikas: Eesti Pank.

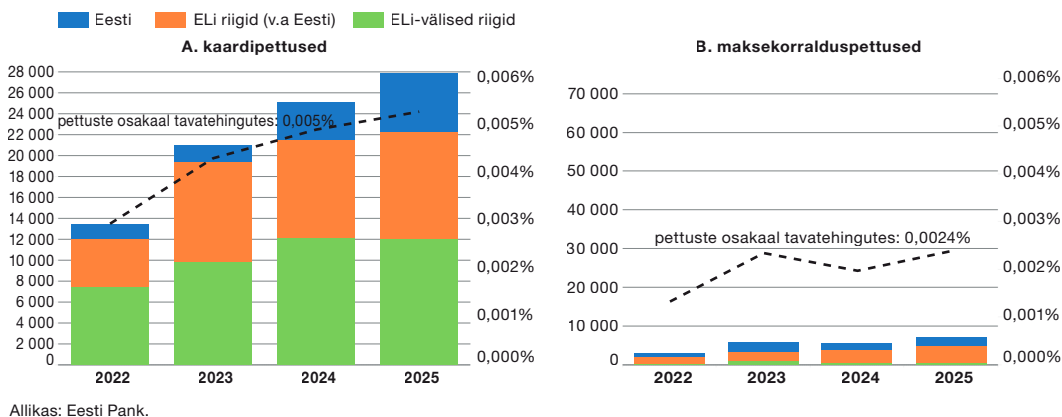
Kogukäibelt võtavad petturid keskmiselt iga makstud 100 euro kohta ümardatult 4 euro senti kaarditehingust (0,037%) ja pool euro senti maksekorraldusest (0,005%). Eriti kaardipettuste puhul on näha, et nii pettuste käibe kui ka tehingute arvu osakaal tavalistes tehingutes kasvab stabiilselt (vt joonised 15 ja 16). Kui 2022. aastal tehti iga 100 000 kaarditehingu kohta kolm kaardipettust, siis 2025. aastal on selleks juba viis kaardipettust (0,005%). Kõige märkimisväärsem on just 2025. aasta kaardipettuste osakaalu tõus tavakäibest, mis on võrreldes 2024. aastaga peaaegu kahekordistunud (0,022%). Maksekorralduspettuste osakaal on püsinud stabiilsena: keskmiselt esineb kaks pettust iga 100 000 maksekorralduse kohta (0,002%; vt joonis 16). Seda tulemust võivad mõjutada ka Eesti elanike suurenenud teadlikkus ning positiivne suundumus, et nii pettusekatsetest kui ka õnnestunud pettustest antakse oma finantsasutusele teada. Samas suurenes 2025. aastal järsult nii ettevõtetele kui

Joonis 15. Pettuste käibe osatähtsus



Allikas: Eesti Pank.

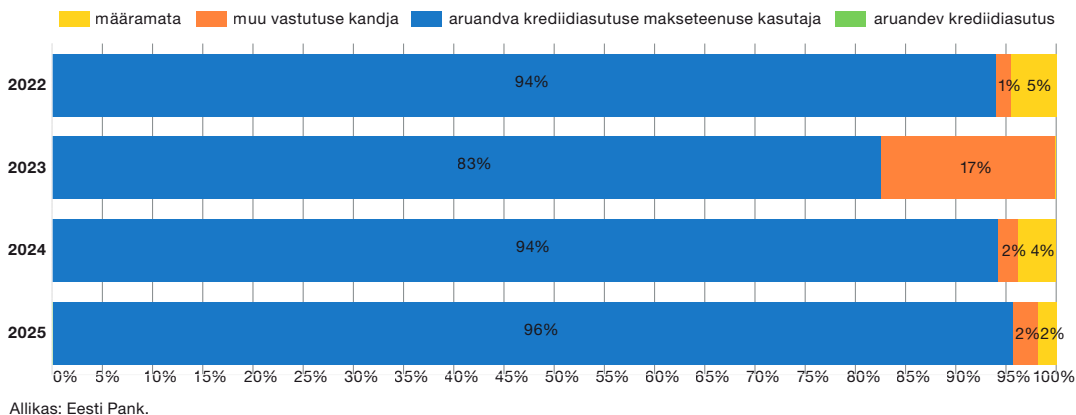
Joonis 16. Pettuslike tehingute osatähtsus



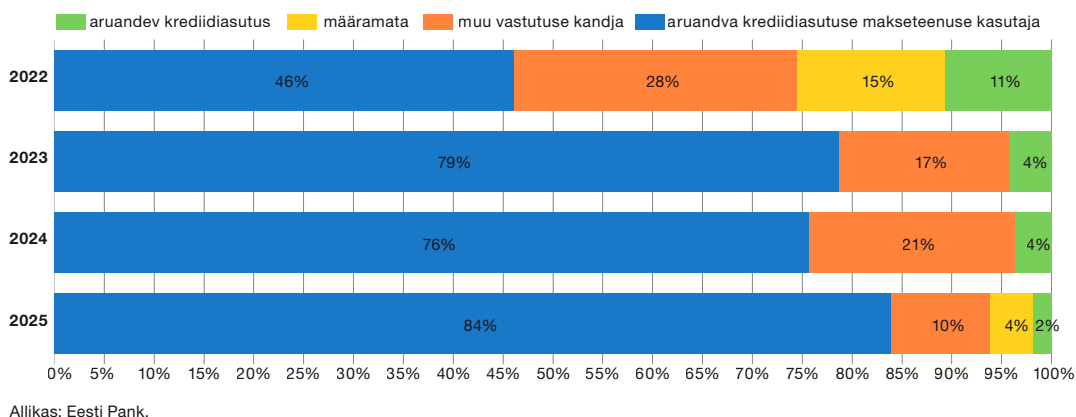
ka erisikutele suunatud maksekorralduspettustega tekitatud kahju. Kuna pettustehingute arv kasvas kahjusummast märksa aeglasemalt, näitab see, et ühe pettuse kohta tekitatud kahju on tunduvalt suurenenud.

Maksekorralduspettuste puhul kannab enamasti ehk 96%-l juhtudest kahju makseteenuse kasutaja ehk klient (vt joonis 17). Peamiseks põhjuseks on raskest hooletusest tulenevad autenditud maksepettused, mille puhul teeb klient ise petturile ülekande või annab talle konfidentsiaalseid andmeid, mis võimaldab kelmil ohvri pangakontot kasutada. Raske hooletuse puhul ei rakendu pangale makseteenuste direktiivist (PSD2) tulenev nõue, mille alusel tuleb kliendile kahju hüvitada. Kaardipettuste puhul jääb kliendi kanda 84% kahjust (vt joonis 18). Veel 10% kahjust kannab muu vastutav osapool, näiteks kaupmees või maksete

Joonis 17. Maksekorralduspettuste kahju vastutaja järgi



Joonis 18. Kaardipettuste kahju vastutaja järgi



vastuvõtja (*acquirer*), kellega kaupmehel on sõlmitud makselahenduse teenuse leping. Ülejäänud 6% on kas määramata vastutusega või jääb panga kliendi kanda. Viimasel juhul hüvitab pank kahju, mida klient pettuse tõttu kandis. Kaardipettuste puhul vaadatakse, kas klient on tegutsenud raske hooletusega ning kas kaupmees on täitnud nõutavaid turvameetmeid, näiteks rakendanud 3D Secure'i. Kui tehing ei ole nõuetekohaselt tugevalt autenditud, siis vastutab pettusliku tehingu kahju eest kaupmees.

Turvalised ostud internetis ehk ametliku nimetusega 3D Secure on täiendav turvameede, mille puhul tuvastatakse kaardiomanik lisaautentimise abil, et vältida kaarditehingutega tehtavaid pettusi veebipoodides.

PETTUSED ERI PIIRKONDADES

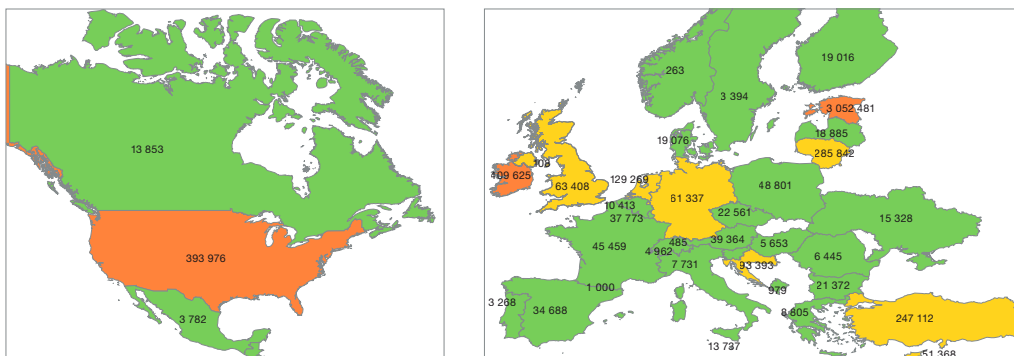
Kaardipettused Eesti pangakaartidega

Eesti pangakaartidega sooritatud pettused saab piirkonna järgi jagada kolmeks: Eestis, mujal Euroopas ja väljaspool Euroopat tehtud pettused. Nende piirkondlik jaotus on esitatud joonistel 15 ja 16. Eestis tehtud kaardipettused põhjustasid 2025. aastal üle poole kogukahjust ehk 56%. Mujal Euroopas tehtud pettuste osa kogukahjust oli 23% ja väljaspool Euroopat tehtud pettustel 21%. Pettuste arvu järgi on statistiline pilt regiooniti siiski väga eriline. Väljaspool Euroopat tehti ligikaudu 12 000 petturlikku kaarditehingut ehk 43% kõigist Eesti pangakaartidega tehtud pettustest. Eestis pandi 2025. aastal toime 5600 kaardipettust ehk 20%, mis on piirkondade võrdluses kõige väiksema osakaaluga. Mujal Euroopas aga sooritati 10 300 pettust ehk 36%. Väljaspool Euroopat ei rakendata kaarditehingutele alati tugeva autendimise nõudeid, mis tähendab, et selliste tehingute puhul on pettuseoht kõige suurem.

Riikide võrdluses põhjustasid Eestis välja antud pangakaartidega kõige rohkem kahju Ameerika Ühendriikides, Iirimaa ja Eestis tehtud petturlikud tehingud (vt joonis 19). Nendes riikides tehti ka arvult kõige rohkem petturlikke tehinguid. Tuginedes Euroopa Keskpanga ja Euroopa Pangandusjärelevalve koostöös välja antud pettuste raporti statistikale, toimub Eesti pangakaartidega sellegipoolest kolm korda vähem kaardipettusi kui mujal Euroopa riikides välja antud pangakaartidega (2024. aasta seisuga, [EKP, 2025](#)).

Joonis 19. Eesti kaardipettuste kahjude jaotus riigiti (eurodes)

■ kolm suurima pettusekahjuga riiki ■ järgmised seitse pettusekahjuga riiki ■ ülejäänud pettusekahjuga riigid



Allikas: Eesti Pank.

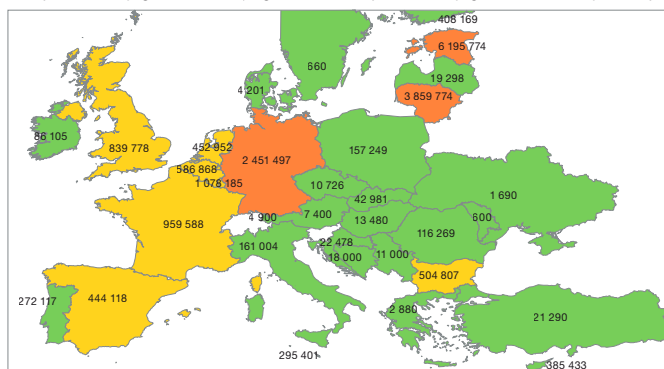
Maksekorralduspettused Eesti pangakontodelt

Eesti pangakontodelt teistele Eesti kontodele tehtud petturlikud maksekorraldused moodustasid pettuste käibest 31% ja arvust 30% (vt joonised 15 ja 16). Kõige suurem osa petturlikest maksetest jõudis mujale Euroopa riikidesse: sinna suunati 59% pettuste käibest ja 62% maksetest. Väljaspool Euroopat asuvatele kontodele jõudis esimese maksena 10% pettuste käibest ja 8% maksetest. Riikide võrdluses jõudis

kõige rohkem raha ohvrite kontodelt esmalt teistele Eesti pankade kontodele. Teisel kohal oli Leedu ja kolmandal Saksamaa (vt joonis 20). Sama jaotus kehtib ka pettuste arvu kohta eelnevas kolmes riigis. Need andmed näitavad, et rahamuuladel on pettuse teel saadud raha vastuvõtmiseks kontod pankades üle kogu Euroopa. Oma klientide parem tundmine aitab seega pankadel petturite takistamiseks täiendavaid meetmeid võtta ja aidata seeläbi maksekorralduspettustest tulenevaid kahjusid ennetada. Samas kasutavad Eesti eraisikud ja juriidilised isikud üha enam ka teistes Euroopa riikides tegutsevate makseasutuste teenuseid, mistõttu ei viita välisriigi kontole raha saatmine iseenesest pettuseriskile. Euroopa Keskpanka ja Euroopa Pangandusjärelevalve raporti järgi on Eesti maksekorralduspettuste osakaal Euroopaga võrreldes keskmisel tasemel.

Joonis 20. Eesti maksekorralduspettuste kahjude jaotus riigiti (eurodes)

■ kolm suurima pettusekahjuga riiki ■ järgmised seitse pettusekahjuga riiki ■ ülejäänud pettusekahjuga riigid



Allikas: Eesti Pank.

MAKSEPETTUSTE TÕKESTAMINE EESTIS

Pettusekatseid tehakse erakordselt palju, kuid suur osa neist ei pruugi inimesteni jõuda. Pettuste tõkestamiseks on teenusepakkujad astunud väga jõulisi samme. Ainuüksi 2026. aasta esimese viie kuuga tõrjus Telia üle 20 miljoni ohu, millest suurema osa moodustasid õngitsuslehed ja halva mainega veebilehed (Telia, 2026). Aasta algusega võrreldes vähenes petukõnede hulk Telia võrgus märgatavalt. Kui jaanuaris tuvastas ja blokeeris Telia üle kahe miljoni petukõnekatse, siis aprillis ainult 223 000 (Telia, 2026). Sarnaseid meetmeid rakendavad ka Elisa ja Tele 2. Elisa blokeeris esimesel poolaastal üle kuue miljoni petukõnekatse ning statistika näitab samuti petukõne katsete vähenemist (Elisa, 2026). Tele2 teatel on petukõned suundumas ettevõtete poole, kelle kahjusummad on suurimad (Tele2, 2026). Sellegipoolest ei suuda tehnilised meetmed kõiki petukõnesid tõkestada. Piisab ainult ühest edukast võltsitud ehk *spoof*itud numbriga tehtud petukõnest ja kahjud võivad nii eraisiku kui ka ettevõtte puhul osutuda äärmiselt suureks.

Spoofing'ut kasutavad kurjategijad kuvavad tehniliste võtetega kõne saaja telefoniekraanile numbri, mis näeb välja nagu Eesti number. Nii on suurem võimalus, et inimene võtab telefonikõne vastu ja usaldab kelmi. Sageli pole numbri omanikud ise teadlikud, et nende numbrit on spoof'itud.

Pangad on juba aastaid kasutanud mitmesuguseid kõrgetasemelisi turvalahendusi. **POS- ja ATM-pettuste** vähendamiseks kasutatakse järgmisi meetmeid:

- EMV-standardile vastav kiibitehnoloogia, mis salvestab andmeid turvaliselt ja genereerib ainulaadseid tehingukoode, tehes kaartide kloonimise ehk skimmimise keeruliseks.
- Sularahaautomaatidesse paigaldatud andurid, mis aitavad tuvastada skimmimisseadmeid.
- Geoblokeerimine ehk võimalus tõkestada kaardi kasutamist väiksema turvalisusega piirkondades.
- Kaupmehi kaitsev vastutuse ülemineku põhimõte (*liability shift*), mille kohaselt võib vastutus petturliku tehingu eest minna kaupmehelt kaardi väljastajale või teisele makseahela osalisele, kui kaupmees on nõuetekohaselt rakendanud klientide kaitseks EMV-tehnoloogiat ja 3D Secure'i.

Internetipettuste (sh pettuslike maksekorralduste) vähendamise meetmed:

- Turvalised internetiostud ehk 3D Secure. Selle rakendamine mängib internetipettuste ennetamises suurt rolli, sest ostu sooritamisel võidakse kaardi valdajalt nõuda isiku täiendavat tuvastamist. Selleks suunatakse ta tavaliselt internetipanga autentimiskeskonda, kus kinnitab tehingu näiteks Smart-ID, Mobiil-ID või muu autentimisvahendiga.
- Tokeniseerimine, mille käigus asendatakse tundlikud kaardiandmed, näiteks kaardi number, digitaalse tähise ega tokeniga.
- Makse saaja andmete ehk nime ja kontonumbri vastavuse kontroll maksetel.
- Pankade pidev tehingute seire, mis põhineb muu hulgas kliendipõhistel riskiskooridel ja käitumismustritel.
- Pankade tehnoloogiliste seiresüsteemide uuendamine ja arendamine.
- Täiendavate autentimisetappide rakendamine kliendi kontole juurdepääsul ja hoiatuste kuvamine uute seadmete ja IPD-aadresside tuvastamise korral.
- Teatud juhtudel piirangute seadmine, näiteks telefonikõne ajal tehingutest keeldumine või suurema riskiga tehingute piiramine.

Politsei tegeleb samuti aktiivselt pettuste ennetamisega. Kelmide elu raskeks tegemiseks tuvastab ja blokeerib politsei nende pangakontosid ja telefoninumbreid ning parandab pidevalt inimeste teadlikkust. See vähendab petturite manipuleerimisvõtete tulemuslikkust.

Finantspettuste tõkestamise ümarlaud

Pettuste ohjeldamiseks kutsus Eesti Pank 2025. aastal kokku finantspettuste tõkestamise ümarlaua, mis ühendab avaliku sektori asutusi ja erasektorit. Ümarlaua peamine eesmärk on tuua kõik asjaosalised ühisesse informuumi, töötada välja ja viia ellu pettuste tõkestamise tegevuskava, teha vajadusel õigusaktide muutmise ettepanekuid jms. Tegevuskava elluviimise eest vastutab Rahandusministeerium ja koosolekuid koordineerib Eesti Pank. Pettuste tõkestamine puudutab mitme ministeeriumi – [Rahandusministeeriumi](#), [Justiits- ja Digiministeeriumi](#), [Majandus- ja Kommunikatsiooniministeeriumi](#), [Siseministeeriumi](#) – ning mitme teise asutuse ja organisatsiooni, sealhulgas [Politsei- ja Piirivalveameti](#), [Eesti Pangaliidu](#), [Eesti Panga](#), [Tarbijakaitse ja Tehnilise Järelevalve Ameti](#), [Prokuratuuri](#), [Riigi Infosüsteemi Ameti](#) ja [Finantsinspektsiooni](#), tegevusvaldkonda. Ümarlaua töösse on kaasatud ka erasektori esindajad, eelkõige pangad, telekommunikatsiooni- ja tehnoloogiaettevõtted, sealhulgas [SALV](#) ja [SK ID Solutions](#), maksevahendajad ning krüptoettevõtted.

Lisaks Eesti Panga juhitud ümarlauale on pettustega võitlemiseks loodud koostöövormid ka Politsei- ja Piirivalveameti ning Eesti Pangaliidu juurde. Erinevatel koostöövormidel on mõnevõrra erinev fookus. Eesmärk on vältida tegevuste dubleerimist ning kujundada selge tööjaotus strateegiliste eesmärkide seadmise ja operatiivsete tegevuste elluviimise vahel.

Olulisemad tegevused ja saavutused ümarlaua tegevuskava elluviimisel ning ümarlaua osalejate algatatud tegevused.

Muudatused seadusandluses

- 2026. aasta suvel jõudis Riigikokku finantspettuste tõkestamise eelnõu, millega antakse makseteenuse pakkujatele õiguslik alus keelduda maksejuhise vastuvõtmisest, kui on alust pettust kahtlustada. Lisaks saavad pangad õiguse jagada andmeid teiste krediidiandjate ja politseiga juhul, kui on kahtlus, et klient või maksetehing on seotud pettusega. Tegemist on väga oluliste muudatustega, kuna puudujäägid infovahetuses on seni olnud vesi petturite veskile. Samuti on oluline, et pangad saavad õiguse peatada kliendi maksetehingu, kui on kahtlus, et klient teeb tehingu petturi mõjutusel. Lisaks muudetakse eelnõuga krediidiandjate ja -vahendajate seadust, et takistada petturi ohvri nimel laenuvõtmist.
- Euroopa Liidus jõuti uues makseteenuste pakettis (uus makseteenuste määrus ja direktiiv) poliitilise kokkuleppeni 2024. aasta novembris. Otsekohalduvas määruses (*Payment Services Regulation*, PSR) on pettusevastastel meetmetel keskne koht. Uus määrus ja direktiiv asendavad senise teise makseteenuste direktiivi (PSD2). Uus määrus näeb ette arvukalt meetmeid pettuste tõkestamiseks. Muu hulgas tekib makseteenuse pakkujatel kohustus blokeerida pettuse kahtluse korral makseid. Samuti peavad nad vahetama pettustega seotud teavet nii omavahel kui ka politseiga. Finantspettuste tõkestamise eelnõus on makseteenuse pakkujatele sätestatud sarnased õigused. Lisaks näeb uus makseteenuste pakett ette, et teatud juhtudel vastutab makseteenuse pakkuja kliendile pettusega tekitatud kahju eest ka siis, kui klient on ise makse kinnitanud. See tähendab, et makseteenuse pakkuja peab inimesele hüvitama selle summa, mille ta pettuse tulemusel kaotas. Määrust hakatakse eeldatavalt rakendama 2028. aasta lõpus.
- Muutmisel on sideteenuste osutamist reguleeriv Vabariigi Valitsuse määrus. Muudatuse eesmärk on kohustada sideteenuste osutajaid rakendama meetmeid petukõnede takistamiseks. Suuremad telekommunikatsiooniettevõtted on need meetmed juba kasutusele võtnud ning investeerinud pettuste tõkestamisse, blokeerides igal kuul miljonid petukõnesid, ootamata selleks regulatiivset kohustust. Pärast määruse jõustumist laieneb meetmete rakendamise kohustus ka väiksematele telekommunikatsiooniettevõtetele. Määrus jõustub 2027. aasta alguses.
- Krüptovaraga tehtud tehinguid hakkab rangemalt reguleerima uus ELi makseteenuste määrus.

Pankade tegevus

Pangad on teinud märkimisväärseid investeeringuid pettuste tõkestamise süsteemidesse ja turvameetmetesse. Suuremad võimalused pettuste tõkestamiseks näeb ette pankadele eespool nimetatud finantspettuste tõkestamise eelnõu. Pangad on koostanud ka pettuste tõkestamise hea tava ja meetmete kava. Hea tava eesmärk on:

1. kirjeldada ühiseid väärtusi, suuniseid ja põhimõtteid, millest pangad pettuste tõkestamisel lähtuvad;
2. suurendada pankade ja ühiskonna teadlikkust pettuste riskidest ning kaitsemeetmetest;
3. edendada tulemuslikku koostööd pettuste tõkestamisel nii pangandussektoris kui ka erinevate sektorite, sh avaliku sektori vahel, arvestades iga panga iseseisvust konkreetsete meetmete valimisel ja rakendamisel.

2026. aasta meetmete kava näeb muuhulgas ette sularaha väljavõtmise ja tehingute limiitide ülevaatamise ning Smart-ID+ kasutuselevõtu. Samuti suurendatakse ettevõtete teadlikkust nelja silma põhimõttest, et soodustada selle laiemat kasutamist maksete tegemisel. Pangaliidu hea tava ja meetmed on kättesaadavad [Pangaliidu kodulehel](#).

Oluline on rõhutada, et kuigi tihti vaadatakse pettuste puhul sageli ennekõike just pankade kui inimeste ja ettevõtete poole, ei vastuta maksepettuste ennetamise eest ainult pangad. Vastutus jaguneb klientide, pankade, riigiasutuste, tehnoloogiaettevõtete, sideoperaatorite ja teiste teenusepakkujate vahel. Pettused saavad sageli alguse juba enne makse tegemist ja väljaspool panka – inimesi petetakse telefoni, sotsiaalmeedia, e-kirjade või võltsitud veebilehtede kaudu. Pangad rakendavad kõiki seadusega ette nähtud meetmeid finantspettuste ennetamiseks ja klientide kaitsmiseks, kuid pettuste ärahoidmisel on määrava tähtsusega inimeste endi tähelepanelikkus ja ettevaatlikkus. Pangad on teada andnud, et nad suudavad praegu tõkestada üle poole pettusekatsetest.

Teavituskampaaniad

- Politsei teeb iga päev teavitustööd, koostab muuhulgas üksikasjalikku pettusjuhtumite statistikat ja on loonud juhendi kuidas ennast kelmide eest kaitsta, mis on leitav [Politsei](#) kodulehel.
- Rahandusministeerium käivitas 2026. aasta suvel koos hanke võitnud partneriga poolteist aastat kestva finantspettuste ennetamise teavituskampaania. Kampaaniaga püütakse jõuda võimalikult paljude Eesti elanikeni, sealhulgas nendeni, kes tavameediat ei jälgi. Selleks kasutatakse muu hulgas välireklaami ja sotsiaalmeediat.
- Hiljuti valmis riiklik finantspettuste ennetamise kommunikatsioonistrateegia, mille peamine eesmärk on suurendada inimeste usku oma suutlikkusse pettusi ära tunda ja neile vastu seista. Strateegia annab suunised sõnumite kujundamiseks nii, et teavitus ei tekitaks liigset ärevust ega õõnestaks inimeste põhjendatud ohutaju. Riigi, aga ka erasektori partnerite sõnumid ja tegevus peavad aitama vähendada pettuse ohvriks langemisega seotud häbitunnet, hoida ühiskondlikku ohutaju ja kinnistada praktilisi käitumisviise pettuse korral. Peamised pettuste ennetamise ja tõkestamisega seotud riigiasutused on Rahandusministeerium, Justiits- ja Digiministeerium, Siseministeerium, Politsei- ja Piirivalveamet, Riigi Infosüsteemi Amet, Tarbijakaitse ja Tehnilise Järelevalve Amet, prokuratuur ja Eesti Pank.
- RIA on ette valmistamas oma kampaaniat, millest saab täpsemalt lugeda nende [kodulehel](#).
- Eesti Pangaliit ja telekomifirmad tegelevad samuti pidevalt pettuste ennetamise kampaaniatega, millega saab lisaks tutvuda Pangaliidu poolt koostatud [pettuseinfo](#) kodulehel.

Pangaliidul on eraldi pettuste tõkestamise toimikond. Samuti algas 2025. aastal pettuste tõkestamise kampaania „Petturil on mitu nägu“, mida aitasid rahastada ka sideettevõtted Telia, Elisa ja Tele2. Laiaulatusliku reklaamikampaania eesmärk on parandada inimeste teadlikkust

petuskeemidest. Kannatanud on erineva haridustaseme, sissetuleku ja vanusega ning ohvreid leidub kõikjal Eestis. Kampaania raames edasiantavad sõnumid enda kaitsmiseks on järgmised:

- Tee kindlaks, kellega räägid ja kuhu infot jagad.
- Ära lase end survestada ega kiirustada.
- Keskendu! Ära vajuta hajameelselt linkidele.
- Kahtlane kõne? Pane toru ära. Sa ei pea midagi põhjendama.
- Veendu, mida oma PIN-koodiga kinnitad.
- Hoia oma andmed ainult enda teada.
- Küsi julgelt kellegi teise arvamust.
- Kui märkad pettust, teavita politseid.
- Kui said petta, teavita oma panka ja politseid.

Pangaliit jätkab ka 2026. aastal erinevate teavituskampaaniate korraldamist, ühendades jõud Rahandusministeeriumi ja PPA ettevõtmistega.

Märkimisväärne on ka RIA tegevus pahavara kohta teabe jagamise platvormi MISP (*Malware Information Sharing Platform*) laialdasemaks kasutuselevõtuks. Platvormi saavad nüüd kasutada ka telekommunikatsiooniettevõtted, mis võimaldab petturlike veebilehtede kohta kiiremini teavet jagada ja neile juurdepääsu tõkestada.

Facebookis levivatest pettuslikest investeerimis- ja muudest reklaamidest ning nendega seotud veebilehtedest saab teatada TTJA-le, kes tegeleb nende kõrvaldamisega.

SK ID Solutions töötab välja muudatuse, mille tulemusel teises asukohas olevasse seadmesse ei saa Smart-IDd teha. Välja on töötatud Smart-ID+, mille saavad oma teenustes kasutusele võtta pangad ja teised e-teenuse pakkujad. Smart-ID+ seob autentimise kindlamalt kasutaja enda algatatud toiminguga.

Pankadele on kiireks teabevahetuseks oluline SALV Bridge'i platvorm, mis võimaldab pankadel ja teistel finantsasutustel vahetada teavet kahtlaste tehingute ning kontode kohta. Nii aitab kiiresti kindlaks teha, kas pettus puudutab ka teisi finantsasutusi.

Eelpool on kirjeldatud vaid osa pettuste tõkestamisega seotud osalistest, tegevustest ja meetmetest. Eesti Pank ja Rahandusministeerium on seadnud eesmärgiks hoida finantspettuste ennetamist riiklikul tasandil järjepidevalt fookuses ja toetada kõikide asjaosaliste koostööd selle probleemi vähendamisel.

Inimene kui peamine pettuste tõkestaja

Kuigi kõik mainitud meetodid on tõhusad, on pettuste tõkestamisel üks tähtsamaid lülisid siiski inimene ise. Enamikku makse- ja kaardipettustest saab ära hoida, kui kõigepealt veenduda, kellele makse tehakse ja kuhu andmed sisestatakse. Kus vähegi võimalik, tuleb kasutada kaheastmelist tugevat autentimist. Pea meeles, et oma PIN-koodi, paroole ja muid tundlikke andmeid ei tohi kellelegi jagada. See kehtib ka siis, kui suhtled pangatöötaja, politseiniku või mõnda muud asutust esindava isikuga, sest ametnikud ei palu kunagi selliseid andmeid avaldada. Kui keegi väidab kõnes, kirjas või vestlusaknas, et sinu pangakonto on ohus, lõpeta suhtlus ja helista panga ametlikule numbrile, mille leiad ise panga kodulehelt. Suur ohumärk on palve laadida alla mõni kaugjuurdepääsu võimaldav rakendus, nagu TeamViewer või AnyDesk, sest need võimaldavad petturil ohvri arvuti enda kontrolli alla võtta. Samuti tuleb olla ettevaatlik, kui keegi avaldab survet tehing kiiresti lõpule viia, sest kiirustades väheneb ohutaju ja võime märgata kahtlasi üksikasju. Nii ei jää ka aega kelleltki nõu või abi paluda.

Veebipoodi külastades, reklaame nähes või telefoni teel suheldes tuleb meele pidada, et kui pakutav toode või teenus tundub liiga hea, et olla tõsi, siis pole see usaldusväärne. Tüüpilised näited on usumatult suured soodustused või lubadus teenida investeringult suurt tootlust. Enne veebilehel andmete sisestamist tasub kontrollida, kas aadress algab tähisega „https://“ ja sisaldab õiget teenusepakkuja nime ilma kirjavigade või tundmatute sümboliteta. Kui helistatakse tundmatult numbrilt, eriti välismaise

suunakoodiga, võib jätta kõne esialgu vastu võtmata ja otsida internetist, kas selle numbri eest on varem hoiatatud. Üldiselt ei tasuks välisriigist tulevaid kõnesid vastu võtta, kui sul ei ole seal asuvate inimestega mingeid suhteid, sest on väga tõenäoline, et helistaja on hoopis petis.

Kui kahtlustad pettust, on kõige tähtsam tegutseda kohe. Blokeeri kaart või sulge konto, salvesta tõendid (nt SMSid ja ekraanipildid) ja teavita nii enda panka kui ka politseid. Kiire tegutsemine suurendab võimalust oma raha tagasi saada ja petturitele jälile jõuda. Pettuse kahtluse korral tasub alati helistada panga, politsei, pakifirma või mõne muu asutuse ametlikule telefonile ja paluda abi. Nii saab vältida paljusid levinud petuskeeme ja vähendada riski, et sinu isikuandmed satuvad valedesse kättesse ja sa kannad rahalist kahju.

Eesti Panga sõnumid avalikkusele maksepettustest hoidumise kohta on järgmised:

- Kui sinuga võetakse rahaasjus ühendust, ära tegutse kohe. Võta aeg maha ja mõtle, kas tegemist võib olla pettusega.
- Pea meeles: pangad ja ametiasutused ei küsi PIN-koode ega ekraanijagamist ning ei suhtle WhattsAppis ega Viberis.
- Ära ava SMSi või e-kirjaga saadetud kahtlaseid linke ega faile.
- Ära anna võõrastele pangakaarti, PIN-koode ega sularaha, isegi siis, kui nad esinevad kulleri või ametnikuna.
- Kui väidetakse, et su konto on ohus, lõpeta kohe kõne ja helista ise panka või politseisse, et väidet kontrollida.
- Sisesta PIN-koode ainult siis, kui algatasid toimingut ise ja tead täpselt, millist toimingut ja miks kinnitad. Eriti tasub ettevaatlik olla kirjakulleri, elektri- või veearvesti vahetamise ja polikliinikusse kutsumise ettekäändel tehtavate kõnede puhul, millega püütakse ohvrit PIN-koodi sisestama meelitada.
- Kui keegi helistab sulle ja palub PIN-koode sisestada, siis on see alati pettus.