TURVALISUSEST JA PETTUSTE ENNETAMISEST

Soovime olla oma klientidele usaldusväärseks partneriks ning teeme kõik endast oleneva, et Sinu andmed oleksid meie juures hoitud. Oleme tänulikud kõigi teavituste eest, mis aitavad meie teenuste turvalisust suurendada. Teavitusi saab esitada telefonil 667 3200 või e-posti teel info@tkmfinants.ee.

Oma tegevuses lähtume järgmistest turvalisuse põhimõtetest:

- ✓ Tuvastame Sinu isiku Partnerkaardi iseteeninduskeskkonnas usaldusväärsete digitaalsete autentimisvahendite abil, milleks on Smart-ID, mobiil-ID, ID-kaart või pangalink. Meil ei ole vaja teada Sinu PIN-koode ega internetipanga kasutajatunnuseid ega Sinu pangakaardi numbrit.
- ✓ Kõik andmesideühendused on krüpteeritud, kasutame TLS-protokolli.
- ✓ Palume Sul regulaarselt oma andmeid uuendada. Nii on meil võimalik tagada Sinu konto turvalisus, takistada pahatahtlikke tegevusi, teavitada kahtlust äratavatest tehingutest ja seeläbi kaitsta Sind võimaliku rahalise kahju eest. Ühtlasi peame krediidiandjana järgima seaduseid, mis on seotud rahvusvahelise rahapesu ja terrorismi rahastamise tõkestamisega.
- ✓ Aitame Sul olla petuskeemidest teadlik. Internetis toiminguid tehes ole tähelepanelik ja hoolas. Oleme oma veebilehele koondanud lühikese ülevaate erinevatest olukordadest, mida Eestis finantspettuste puhul kõige sagedamini kasutatakse. Võta aega nendega tutvumiseks, et teaksid, kuidas ennast petturite eest kaitsta.

Enimlevinud finantspettused

„Pangapettus“

Sinu poole pöördutakse kas e-kirja, SMSi, Messengeri vestluse või telefoni teel ning esinetakse TKM Finants ASi, Kaubamaja või Selveri töötajana. Sind võidakse suunata veebilehele, mis näeb Partnerkaardi lehega äravahetamiseni sarnane välja, ja pettur võib Sinult küsida näiteks pangakaardi ja selle CVV-numbrit, Sinu internetipanga kasutajatunnust või Sinu isikukoodi ja PIN-koode. Samuti võidakse Sinult küsida infot Partner Kuukaardi makselahendustega sooritatud tehingute kohta vms teavet. Pärast info kogumist võidakse sõltuvalt andmetest kasutada neid Sinu internetipanka sisselogimiseks ja Sinu arvelt ülekannete tegemiseks, Sinu nimel krediidilepingute sõlmimiseks või ka Partner Kuukaardi makselahenduste kasutamiseks e-poodides jne. Samuti võidakse Sinult saadud teavet kasutada selleks, et esitada Sulle meie nimel arveid, kuid makse saajaks on pettur märkinud enda pangakonto.

„Arvepettus“

Petturid saadavad Sulle TKM Finants ASi nimel arve teenuste või kauba eest, mida Sa pole tellinud/ostnud. Samuti võib juhtuda, et arve esitatakse teenuse või kauba eest, mida Sa oled tegelikkuses ka tarbinud, kuid makse saaja pangakonto erineb meie omast. Pettur loodab, et Sa ei kontrolli arvet ja teed ülekande.

„Õnneloosipettus“

Petturid loovad sotsiaalmeediaplatvormidel (Facebook, Instagram, Twitter) tuntud ettevõtte nimel libakonto ning loovad postituse, mille sisuks on atraktiivse auhinna loosimine. Nt Selver loosib välja 100-eurose ostukorvi terveks aastaks või Kaubamaja paneb välja 1000-eurose kinkekaardi.

Samuti võidakse ohvrile saata e-kiri või sotsiaalmeedia kaudu sõnum, kus väidetakse, et ta on võitnud auhinna, vaatamata sellele, et ta pole mängus/kampaanias isegi osalenud.
Kui ohver reklaamile klõpsab, palutakse esitada isikuandmed, teha makse, sisestada pangakonto või pangakaardi number jne. Pärast teabe kogumist võidakse sõltuvalt andmetest neid kasutada Sinu internetipanka sisselogimiseks ja Sinu arvelt ülekannete tegemiseks, Sinu nimel võidakse sõlmida krediidilepinguid, kasutada Partner Kuukaardi makselahendusi jne.
Samuti võidakse lingile klõpsamisega Sinu seadmesse paigaldada pahavara, mis edaspidi kõiki Sinu tegevusi jälgib ning Sinu isikuandmeid ja finantsinfot salvestab.

„Romantikapettus“

Kohtumine kelmiga toimub veebis, näiteks sotsiaalmeedias või tutvumisportaalis, kus pettur esineb valenimega. Petturid on väga aktiivsed suhtlejad, nende eesmärk on Sinus kiiresti suuri ja sügavaid tundeid tekitada, et Sinu üle kontroll saavutada. Üsna pea pärast tutvumist paluvad petturid Sinult rahalist abi, põhjendades seda näiteks ootamatu töökaotuse, õnnetuse, luhtunud ärivõimaluse või oma lähedase abistamisega. Rahaline abi võib seisneda näiteks ka selles, et pettur palub Sul Kaubamajast mõne Partner Kuukaardi makselahendusega osta köögitehnikat või muid kaupu. Kui Sa seda ei tee, võivad nad Sind hakata ähvardama, kasutades ära teievahelisi intiimvestluseid. Selline manipulatsioon on sageli korduva iseloomuga.

Kasulikke nõuandeid

- ✓ Hoia Partner Kuukaardi ostulimiidi PIN-kood teistele kättesaamatus kohas. Pea meeles, et rahakott ei ole PIN-koodi hoidmiseks turvaline koht.
- ✓ Kui Sinu poole pöördutakse telefoni, e-posti või suhtlusrakenduse kaudu, esinedes mõne panga, Kaubamaja, Selveri, TKM Finantsi või Partnerkaardi töötajana, ning Sinult küsitakse näiteks pangakaardi numbrit, salasõnu, PIN-koode või muud tundlikku finantsinfot, katkesta viivitamatult suhtlus ning teavita meid sellest telefonil 667 3200 või e-posti aadressil info@tkmfinants.ee.
- ✓ Kui kahtlustad, et tegu võib olla pettusega, küsi üle, kellega nad rääkida soovivad. Petukõne puhul reeglina helistaja ei tea, kelle numbrile nad parasjagu helistavad.
- ✓ Veendu, et Partnerkaardi veebilehe aadress on veebilehitsejasse sisestatud õigesti ja sa kasutad turvalist ühendust. Veebileht peab kuvama tabaluku märki ja sellel klõpsamisel kuvama teadet „*Connection is secure*“. Kui veebilehitseja teavitab sind ühenduse võimalikest turvalisuse- või sertifikaadiprobleemidest, hoidu veebilehe kasutamisest.
- ✓ Uuenda nii oma telefonis kui ka arvutis tarkvara ja tee turvauuendusi korrapäraselt.
- ✓ Võimaluse korral paigalda oma seadmetesse viirusetõrje tarkvara.
- ✓ Hoia oma internetipanga kasutajatunnus, parool ja autentimisvahendite PIN-koodid ainult enda teada. Pea meeles, et ei pangad ega meie ei küsi Sinu paroole ega PIN-koode mitte kunagi ei e-posti ega telefoni teel.
- ✓ Mobiil-ID-d ja Smart-ID-d kasutades veendu alati, et Sinu mobiiltelefonis kuvatav kontrollkood vastab internetipangas või mobiiliäpis näidatud koodile. Mobiil-ID ja Smart-ID PIN-koode tohid sisestada ainult oma mobiiltelefoni vastavas rakenduses. Mobiil-ID ja Smart-ID PIN-koode ei tohi kunagi sisestada veebilehtedele, sh internetipangas või Partnerkaardi iseteeninduskeskkonnas!
- ✓ Partnerkaardi iseteeninduskeskkonda sisse logides kasuta alati PIN1-koodi. Kui selleks küsitakse Sinult PIN2-koodi, siis katkesta kohe sisselogimine ja teavita meid juhtumist.
- ✓ Ole isiklikku informatsiooni tuttavatega (eriti internetituttavatega) jagades ettevaatlik. Seda teavet võidakse kasutada sinu manipuleerimiseks.
- ✓ Kui võimalik, kontrolli veebituttava tausta (nt Google’i abiga). Kui sul on inimese identiteedi suhtes kahtlusi, lõpeta suhtlus.
- ✓ Kui oled langenud pettuse ohvriks, võta kohe ühendust politseiga. Kui oled petturi palvel raha üle kandnud, teavita sellest ka oma panka. Anna meile teada mistahes juhtumitest, kus Sinult on

palutud Partner Kuukaardi makselahenduste kasutamist teise isiku hüvanguks, või avastad, et Sinu andmeid on Sinu tahte vastaselt kasutatud Partner Kuukaardi lepingute sõlmimiseks.

- ✓ Ole ettevaatlik tundmatult aadressilt saadetud e-kirjade või tundmatult numbrilt saadetud SMS-ide suhtes. Kontrolli alati õigekirja ja grammatikat – vead osutavad petusõnumile. Ära kunagi ava kahtlase e-kirja või sõnumiga saadetud linke.
- ✓ Suhtu väga ettevaatlikult sõnumitesse, milles väidetakse, et oled midagi võitnud, kui tead, et pole võitmiseks midagi teinud. Ära kunagi ava selliste sõnumitega saadetud linke.
- ✓ Toodete või teenuste eest arve saamisel e-posti teel kontrolli alati üle, kas saaja pangakonto number kattub teenuseosutaja või müüja ametlikul veebilehel toodud kontonumbritega. TKM Finants ASi kontonumbrid leiad Partnerkaardi iseteeninduskeskkonnast www.partnerkaart.ee.