Veebipõhised finantspettused ja kelmused tehisaru maailmas

OLE VALVEL JA KAITSE ENNAST

Veebipõhised finantspettused ja kelmused ei ole uued, kuid tehisintellekt on muutnud need targemaks ja raskemini avastatavaks. Kurjategijad kasutavad nüüd valesõnumeid ja veebisaite, võltsitud kuulsuste profiile ja isegi tehisaru loodud hääli või videoid, mis näevad välja nagu sinu panga töötaja, sinu sõbrad või perekond – kõige selle eesmärk on sind petta.

Sageli jõuavad nad sinuni sotsiaalmeedia, sõnumirakenduste, e-kirjade ja ootamatute kõnede kaudu, mis näivad ehtsad.

Võid puutuda kokku rahaline kahju, identiteedivarguse ja emotsionaalse stressi ohuga. Ole ettevaatlik ja järgi neid peamisi näpunäiteid, et sul oleks ohutu:

Ole valvas tehisintellektil põhinevate veebipõhiste finantspettuste ja kelmuste suhtes,
nt kellegi teisena esinemine, andmepüük, investeerimis- ja kindlustuspettused ning isegi armukelmused ja-pettused. Saada rohkem teavet eri liiki pettuste ja kelmuste kohta vt lk 5, 6, ja 7.

Ning krüptole omaste pettuste ja kelmuste kohta ( ).

Pane tähele ohumärke:
õpi kahtlast käitumist, sõnumeid või pakkumisi ära tundma (vt lk 2).

Kaitse ennast:
kaitse oma isikuandmeid (vt lk 3) ja

Tea, mida teha, kui satud pettuse või kelmuse ohvriks
(vt lk 4).

Ohumärgid

Lubadus, mis tundub liiga hea, et olla tõsi.

Ootamatu kõne tundmatult numbrilt.

Kiireloomuline taotlus raha või isikliku teabe saamiseks, sealhulgas kelleltki, kes teeskleb, et on pereliige, sõber või isegi avaliku elu tegelane.

Taotlus sinu seadme üle kontrolli võtmiseks, rakenduse allalaadimiseks, QR-koodi skannimiseks või lingil klõpsamiseks.

Isikuandmete või pangaandmete (nt paroolid, krediitkaardi numbrid, internetipanga andmed või turvakoodid) päring.

Taotlus maksete tegemiseks jälgitamatuid teid kaudu (nt krüptod, kinkekaardid, pangaülekanded või ettemakstud deebetkaardid).

Kahtlane või vale e-posti aadress või link (nt kirjavead URL-is või ebatavalised veebiaadressid).

Manus tundmatust allikast, näiteks.exe, .scr, .zip või makrotoega Office'i fail (.docm, .xlsm).

Halb grammatika või vormindamine ametliku välimusega dokumendis, kuigi tehisintellekt võib võimaldada petturitel neid puudusi tõhusamalt varjata.

Veebisait, mis näeb välja professionaalne, kuid millel puuduvad kontrollitud kontaktandmed või ettevõtte registreerimise teave.

Intonatsioon, mis kõlab ebaloomulikult, ei pea pause ja tundub liiga ladus või robotlik. Ole valvel hääle kloonimise suhtes, kuigi tehisaru loodud kõne võib tunduda ka väga loomulik.

Videod, kus hääl võib tunduda robotlik või liiga sujuv, huulte liikumine ja näoilmed võivad olla kõnega halvasti kooskõlas või taust, valgustus ja varjud vastuolulised. Need on sageli tehisaru loodud videod (süvavõltsingud).

Sammud enda kaitsmiseks

1 **Ära kunagi jaga isiklikku või pangateavet:**

Seaduslikud ettevõtted ei küsi kunagi sinu PIN-koode, paroole, internetipanga õigusi ega turvakoode e-posti, teksti, sotsiaalmeedia või telefoni teel.

2 **Peatu ja mõtle, enne kui tegutsed:**

Ära kiirusta raha saatmisega, teabe jagamisega või linkidel klõpsamisega – petturid tekitavad teadlikult kiireloomulisuse tunde (nt IT-probleemid sinu pangaga, hädaabikõned, mis hõlmavad sinu sõpru ja pereliikmeid, ähvardav keelekasutus jne). Kahtluste korral, isegi kui need on väikesed, ära tee midagi; lõpeta kõne ja kontrolli hoolikalt allikat või identiteeti.

3 **Kontrolli allikat/identiteeti tähelepanelikult:**

- Kontrolli alati, kust sõnumid, kõned, e-kirjad ja lingid tulevad- isegi kui need näevad välja ametlikud, pärineda sõbralt või pereliikmelt või isegi avaliku elu tegelaselt. Näiteks helista või saada sõnum oma perele ja sõpradele, kasutades usaldusväärse kanali kaudu teada olevat numbrit; otsi õigekirjavigu, kummalisi URL-e või puuduvaid turvaindikaatoreid (nt veendu, kas veebisaidi link sisaldab HTTPS-is s-tähte, et veebisait oleks turvaline ning kontrolli, kas ettevõtte nimes on täiendavaid või puuduvaid tähti).

- Ära ava linke soovimatutest sõnumitest, lae alla ametlikke rakendusi vaid usaldusväärsetest kauplustest ning ära skanni tundmatuid QR-koode.

- Lepi oma perega kokku turvasõna ehk salajane fraas, mida saate kasutada identiteedi kinnitamiseks, kui tuttav hääl kiireloomulise rahataotlusega helistab ja väidab, et oled tema pereliige (nt vanemad, õde/vend, laps).

- Kasuta kontrollitud kontaktandmeid, et jõuda otse ettevõtte või üksikisikuni ja ära kunagi tugine kahtlustatava petturi esitatud kontaktandmetele (nt otsi ettevõtte nimi ise üles, kasuta ametlikke äriregistreid ja varem kinnitatud kontaktviise). Petturid võivad väita, et neil on tegevusluba või jäljendada loaga ettevõtte veebisaiti. Kontrolli, kas sinu riigi finantsjärelevalveasutus on väljastanud hoiatusi või kas need on kantud IOSCO I-SCANi nimekirja (iosco.org/i-scan/). Krüptoteenuse osutajate puhul veendu, kas neil on ELis tegevusluba (nt kontrolli ESMA registrit ( ).

4 **Pööra tähelepanu võimalikele tehisaru trikkidele:**

Tehisaru tehnoloogia arenedes muutuvad pettused veenvamaks kui kunagi varem, isegi parimate turvameetmete korral. Kui miski tundub ebatavaline või kui märkad mõnda eespool kirjeldatud ohumärki, peatu ja hinda olukorda.

5 **Ära kunagi installi kaugjuurdepääsu tarkvara ega jaga oma ekraani:**

Pangad ja finantsasutused ei nõua seda kunagi.

6 **Hoia seadmed ja kontod turvalisena:**

Kasuta tugevaid ja kordumatuid paroole, hoia neid salajas ja väldi samade paroolide kasutamist erinevatel platvormidel. Luba võimaluse korral mitmikautentimine. Vaata mõningaid paroolide soovitusi siit ( ). Hoia oma tarkvara ja viirusetõrje ajakohased ning aktiveeritud.

7 **Ole ettevaatlik ootamatute ja piiratud aega kestvate investeerimisvõimalustega:**

Kui see kõlab liiga hea, et olla tõsi, see ilmselt see nii ka on.

8 **Mõtle enne, kui jagad sotsiaalmeedias teavet:**

Vestlusrühmad, foorumid, sotsiaalmeedia postitused ja fotod võivad olla petturitele väärtuslikud teabeallikad. Liiga palju enda või oma investeeringute kohta paljastamine võib muuta sind kergeks sihtmärgiks.

Mida teha, kui oled langenud pettuse või kelmuse ohvriks

Peata tehingud kohe,

Et blokeerida kõik edasised ülekanded kahtlastele kontodele ja vältida täiendavaid kahjusid. Lõpeta kõik kontaktid petturitega – eira nende kõnesid ja e-kirju ning blokeeri saatja.

Võta ühendust oma panga või finantsettevõttega:

Teavita oma panka või finantsettevõtet kohe ametlike kontaktkanalite kaudu, et uurida tehingute külmutamiseks või tagasipööramise võimalusi.

Muuda oma paroolid kõigis seadmetes ja rakendustes/veebisaitidel.

Petturid ostavad internetis lekkinud paroole ja proovivad neid mitmel kontol. Ainult ühe salasõna muutmisest ei piisa; Veendu, et muudad neid kõiki, nii et petturid ei saaks neid uuesti kasutada.

Teavita ja hoiata:

Teata juhtumist politseile või oma riiklikule finantsjärelevalveasutusele (https://www.fi.ee) ja teavita oma võrgustikku (nt sõpru ja pereliikmeid), et suurendada teadlikkust. See on parim viis ennast ja teisi kaitsta.

Hoidu täiendava pettuse eest:

Pettur võib teie kui varasema pettuse ohvriga ühendust võtta, väites, et ta on avaliku sektori asutus (nt politsei, maksu- või järelevalveasutus) ning pakkuda teie kaotatud raha tasu eest tagasi. See on sageli järjekordne katse sind petta. Pea meeles: see, et sind on üks kord petetud, ei takista sul uuesti ohvriks langemast.

Euroopa Pangandusjärelevalve, Euroopa Kindlustus- ja Tööandjapensionide Järelevalve, Euroopa Väärtpaberiturujärelevalve, 2025

Luxembourg: Euroopa Liidu Väljaannete Talitus, 2025

Taasesitamine on lubatud tingimusel, et viidatakse allikale.
Illustrations: © Nadezhda Buravleva / madedee / Orapun- StockAdobe.com.

PDF ISBN 978-92-9407-212-2 doi:10.2853/3932221 DZ-01-25-100-ET-N

Tehisarul põhinevad veebipõhised finantspettused ja kelmused

Kellegi teisena esinemise pettus ja süvavõltsingu kasutamine

Saad ootamatu kõne kelleltki, kes väidab end olevat pank, avaliku sektori asutus (nt politsei, maksu- või finantsasutus jne), kindlustustoodete turustaja, IT-ettevõte või isegi pereliige. Helistaja võib kutsuda sind üles raha üle kandma, et seda turvaliselt hoida, viidates kahtlasele tegevusele sinu kontol või kindlustuspoliisis. Samuti võidakse sul paluda avaldada oma pangaandmed (nt maksekaardi number, internetipanga andmed või paroolid), klõpsata lingil või installida tarkvara, väites, et see suudab probleemi kiiresti lahendada. Helistaja võib kasutada võltsitud numbrit, mis sageli vastab sinu panga telefoninumbrile, et näida õiguspärane (*spoofing*).

Petturid võivad tehisaru abil luua võltsvideoid, -pilte või-heli, mis jäljendavad kellegi häält (nt pangatöötaja või pereliige), nägu (nt kuulsus) või liigutusi. **Seda nimetatakse süvavõltsinguks.**

Mis võib juhtuda:

Mainides isikuandmeid ja tekitades kiireloomulisuse tunde, meelitab pettur sind tegema toiminguid, mida sa ei kavatsenud teha – näiteks saatma raha oma kontole, klõpsama pahatahtlikul lingil või laadima oma seadmesse pahavara. See võib anda petturile otsese juurdepääsu sinu pangaandmetele. Selle teabe abil saavad nad muuta sinu parooli, pääseda juurde sinu pangakontole ja varastada sinu raha. Pea meeles: see, et helistaja teab sinu isikuandmeid, ei tähenda, et ta on usaldusväärne.

Andmepüük ja manipuleerimisrünne

Sulle saadetakse e-kiri või sõnum, mis näib pärinevat pangast või finantsettevõttest ning hoiatab sind kahtlase tegevuse eest sinu kontol. Logo, paigutus ja keel näevad välja professionaalsed ning sõnum võib ilmuda samal lõimel nagu teised sinu panga vestlused. Sõnum kutsub sind üles klõpsama lingil, et kinnitada oma konto või lähtestada oma parool. Link viib võltsitud veebisaidile, mis näeb sinu internetipangaga identne välja. Ilma arugi saamata sisestad oma andmed veebisaidile, mis on mõeldud sinu isikuandmete varastamiseks.

Petturid kasutavad tehisaru veenvate andmepüügisõnumite koostamiseks, analüüsides ohvrite tuvastamiseks sotsiaalmeedia andmeid ja kohandades sisu iga sihtmärgi jaoks.

Mis võib juhtuda:

Pettur pääseb ligi sinu pangakontole ja varastab sinu raha või loob pettuse toimepanemiseks sinu isikuandmetega võltsprofiili.

Investeerimis- või kindlustuspettus

Näed sotsiaalmeedias või veebisaidil reklaami, milles kuvatakse tuntud ettevõtte pakutavat piiratud aega kestvat investeerimisvõimalust, millega kaasnevad väikesed riskid või piiratud aega kestvat allahindlust. Kuulutusel on kuulsuse foto ja soovitused, mis on sageli võltsitud. Pärast huvi väljendamist lingil klõpsates või vormi täites võetakse sinuga ühendust ja suunatakse sind platvormile või sõnumikanalisse, kus saad professionaalset nõu ja dokumente. Sind julgustatakse investeerima väikest summat, millele järgnevad suuremad summad, või maksma lisatasu näivalt turvalise konto eest.

Petturid kasutavad tehisaru vahendeid, et muuta need võltsitud ettepanekud või e-kirjad väga veenvaks ja raskesti tuvastatavaks. Samuti kasutavad nad tehisarul põhinevaid sotsiaalmeedia programme, et luua võltskontosid, mis sinuga suhtlevad, väärinfot levitavad ja tegelikku käitumist simuleerivad, et luua usaldust ja mõjutada sinu otsuseid.

Mis võib juhtuda:

Pärast raha välja võtmist või nõude esitamist lõpetab kontaktisik vastamise. Avastad, et seda ettevõtet ei ole olemas või et kindlustatud risk ei ole kaetud. Seejärel saad sa aru, et oled petuskeemi osana saatnud raha otse kelmidele. Kahjuks ei saa sa oma raha tagasi ning sinu isiklikke ja rahalisi andmeid saab kasutada edasiste pettuste toimepanemiseks (nt lepingute sõlmimine sinu nimel, mis võib põhjustada veelgi suurema summa kaotamise).

Armukelmused ja petuskeemid

Sinuga on sotsiaalmeedias, tutvumisrakendustes või telefoni/teksti teel ühendust võtnud keegi, keda sa pole päriselus kohanud. See isik võib vestelda sinuga sagedasti, isiklikel ja romantilistel teemadel, luues võltsitud profiilide abil usaldust. Järk-järgult juhib ta vestluse rahaliste võimaluste poole, väites tohutut kasumit krüptoinvesteeringutest ja julgustades sind suure tulu ja madala riski lubadustega investeerima. Isik palub sul kanda raha kontole või juhendab sind konto loomise ja esmase väikese sissemakse tegemisel, et muuta skeem usutavaks, enne kui julgustab sind investeerima rohkem.

Petturid kasutavad tehisaru, et luua võltsprofiile, tuvastada oma ohvreid sotsiaalmeedias/ tutvumisrakendustes, kasutades sinu kättesaadavaks tehtud andmeid, või kasutada sõnumite genereerimiseks juturoboteid.

Mis võib juhtuda:

Pettur kogub nii palju raha kui võimalik, seejärel katkestab suhtluse ja kaob. Võltsitud investeerimisveebisait või -rakendus eemaldatakse võrguühenduseta, jättes sulle juurdepääsu väidetavatele investeeringutele. Mõnel juhul võivad petturid kasutada pettuse käigus saadud teavet sinu sõprade ja perekonna sihikule võtmiseks ning identiteedivarguse toime panemiseks, millel võivad olla sulle rahalised või õiguslikud tagajärjed (nt pettur võib sinu nimel kinnitada varastatud rahakotte ja sind võidakse pidada vastutavaks sinu nime all toime pandud võlgade või kuritegude eest, kuni ei ole tõendatud vastupidist).

Ostupettus

Sa kohtad huvitavat pakkumist ostu sooritamiseks internetipõhises kauplemiskohas. Tehingut pakkuv ettevõte taotleb makset väljaspool ametlikku platvormi, väites, et kasutab turvalist maksesüsteemi, ja saadab sulle ostu lõpuleviimiseks lingi. Link suunab sind petturliku panga autentimise lehele, mis jäljendab panga ametlikku veebisaiti ning kasutab selle logo ja kujundust, nii et sisestad makse tegemiseks oma internetipanga andmed.

Petturid kasutavad tehisaru väga veenvate võltspankade veebisaitide, tellimuste kinnituste ja arvete loomiseks. AI aitab neil jäljendada pärisettevõtete tooni, brändingut ja stiili. Mõnel juhul kasutavad nad AI juturoboteid, et vastata küsimustele ja muuta tehing usutavamaks.

Mis võib juhtuda:

Kolmanda isiku lingi kaudu tehtud makse läheb kauplemiskoha kaitsest mööda. Pettur saab sisselogimisteabe sinu pangakontole ja varastab sinu raha.