5 ohumärki, mis reedavad salakavala petukõne sekunditega

4 kuud tagasi - 26.06.2026 Autor: AM

Usaldus on muutunud kurikaelte kõige väärtuslikumaks valuutaks. Ainuüksi tänavu esimeses kvartalis blokeeris sideoperaator Elisa 5,6 miljonit petukõne katset. Kuigi kaitse on tugev, libiseb osa kõnesid siiski pragudest läbi ja üha sagedamini kuritarvitatakse just Elisa nime. Kuidas aga tunda ära, et toru teises otsas pole mitte abivalmis klienditeenindaja, vaid hoopis küberpätt? Kuidas sellist petukõnet avastada, selgitab Elisa infoturbejuht Mai Kraft.

Kui tuntud kaubamärk on vaid Trooja hobune

Viimaste kuude jooksul on politsei registreerinud mitu ehmatavat juhtumit, kus kelmid on esinenud Elisa töötajatena. Ühel juhul helistati 89-aastasele mehele ning väideti, et tegemist on Elisa ja politsei esindajatega. Petturite psühholoogilise mõjutuse tulemusena andis mees kahel korral tema juurde koju tulnud võõrale inimesele üle sularaha ja kulda. Kahjusumma ulatus šokeeriva 84 000 euroni.

Teises juhtumis teatati mehele väidetavalt Elisa nimel, et tema nimele on avatud mitu kontot ja tekkinud on võlg. Seejärel kaasati vestlusesse näitlejad, kes esinesid pangatöötajate ja politseinikena, juhendades meest muutma pangalimiite ning kinnitama Smart-ID tehinguid.

Elisa infoturbejuht Mai Kraft paneb kõigile südamele, et tuntud ettevõtte nimi on kelmidele vaid mugav ukselink, millest kinni haarata:

> „Kui inimene kuuleb telefoni teel Elisa nime, kipub ta kõnet automaatset usaldama. Just sellele kelmid panustavadki. Tegelikult ei ole nende eesmärk enamasti seotud mobiiliteenuse või telefonilepinguga, vaid inimese pangakonto, identiteedi või rahaga.“

Viis märki, et helistaja ei ole tegelikult Elisa töötaja

Kõige tõhusam relv petturite vastu on teadmised. Siin on viis peamist ohumärki, mis peaksid su peas punase tule põlema panema juba vestluse esimestel minutitel.

1. Kõne algab Elisana, kuid tüüritakse panganduse teele

Kelmid võivad alustada juttu süütust teemast – näiteks väidetavast sideteenuse võlast või sinu nimele avatud kontodest. Mõne minuti möödudes on aga fookus nihkunud mobiiliteenuselt sinu pangakontole ja rahalistele tehingutele. Samuti võidakse sind suunata iseteenindusse sisse logima, kuid tegelikult on tegu pettuseks loodud libalehega, mis näeb välja nagu ametlik portaal. see on nagu eksitav silt linnatänaval, mis juhatab sind otse pimedasse kangialusesse.

> „Kui kõne algab mobiiliteenusest, kuid liigub pangakontode, laenude või rahateemade juurde, tasub olla väga ettevaatlik,“ ütles Kraft.

2. Algab "spetsialistide" teatejooks

Tõelises petukõnes hargneb sageli lahti terve teatrietendus. Kui sa ei neela esimest sööta alla, ühendatakse sind järgmise „spetsialistiga“. Vestlusesse võivad järjest sekkuda väidetav tehniline tugi, pangatöötaja, Eesti Panga esindaja või isegi politseinik.

See mitme osalejaga skeem on nagu oskuslikult lavastatud etendus, mille eesmärk on jätta mulje ametlikust ja kriitilisest menetlusest. Teie ümber luuakse illusioon autoriteedist, et panna teid tegema samme, mida te tavapäraselt kunagi ei astuks.

3. Digitaalse allkirja väljapressimine: Smart-ID ja Mobiil-ID võrgud

Üks kurikaelte levinumaid võtteid on manipuleerida ohver sisestama oma Mobiil-ID või Smart-ID koode. Meeles tuleb pidada kuldreeglit: PIN2-kood on võrdne sinu omakäelise allkirjaga.

> „Ükski Elisa töötaja ei küsi telefoni teel Smart-ID või Mobiil-ID PIN2-koode ega palu nende abil tehinguid kinnitada,“ rõhutas Kraft.

Kui keegi nõuab telefoni teel, et te sisestaksid oma ekraanile ilmuva kontrollkoodi peale PIN2-koodi, allkirjastad juba tõenäoliselt parasjagu oma raha ülekandmist pätile või uue laenulepingu sõlmimist. Sellisel juhul tuleb kõne kohe lõpetada.

4. Tehislik ajahäda ja hirmutaktika

Kelmid on ka head psühholoogid. Nad püüavad sind veenda, et sinu konto on vahetus ohus, keegi võtab parajagu sinu nimele laenu või et käimas on salajane

politseioperatsioon. Miks?

Sest hirmunud inimene on kergesti juhitav. See on nagu kunstlikult tekitatud tulekahjupaanika – kui sulle karjutakse, et maja põleb, jooksed sa uksest välja ega hakka kontrollima, kas kuskilt üldse suitsu tuleb.

> „Kui inimene viiakse hirmu või ärevuse seisundisse, on tal keerulisem kriitiliselt mõelda. Just sellele petturid loodavadki," ütles Kraft.

5. Absurdsed palved, millel puudub seos sideteenustega

Viimane ja kõige selgem ohumärk on see, kui "Elisa töötaja" palub sul teha midagi, mis ei liitu kuidagi telekomiteenustega. Nende palvete hulka kuuluvad pangakonto limiitide muutmine, laenu võtmine, kiirülekannete tegemine, ekraani jagamise rakenduste (nt AnyDesk) paigaldamine, videokõnes osalemine või – nagu hiljutised juhtumid näitavad – sularaha ja kulla üleandmine.

> „Elisa ei saada töötajaid klientide kodudesse raha või väärisesemeid vastu võtma. Samuti ei palu Elisa klientidel oma raha teisele kontole üle kanda," rõhutas Kraft.

Sinu parim kaitse on punane nupp

Kui telefonikõne tekitab sinus kas või kübeme jagu kahtlust, ei tasu jääda viisakaks. Katkesta kõne otsustavalt punast kõne lõpetamise nuppu vajutades. Kui soovid olukorda kontrollida, otsi ise ettevõtte või panga ametlikult kodulehelt klienditoe number ja helista neile tagasi.

> „Kuigi blokeerime iga päev suure hulga petukõnesid, ei ole võimalik kõiki pettusekatseid tehniliselt peatada. Seetõttu on kõige olulisem kaitse inimese enda tähelepanelikkus. Kui kõne tekitab ärevust, nõuab kiireid otsuseid või puudutab ootamatult teie rahaasju, lõpetage kõne ning kontrollige info õigsust ametlikust kanalist," võtab Kraft teema kokku.

Jäta meelde ja pane toru ära, kui helistaja:

- Küsib Smart-ID või Mobiil-ID PIN-koode tehingute või toimingute kinnitamiseks.
- Räägib vajadusest kanda raha "turvalisele kontole".
- Soovitab sul võtta laenu või muuta pangalimiite.
- Ühendab sind kõne siseselt väidetava politsei või pangatöötajaga.
- Avaldab sulle survet ja nõuab kiireid otsuseid.
- Soovib, et annaksid kullerile või "ametnikule" üle sularaha või väärisesemeid.

- Lahendused

- Turvalisus

Pilt

