5 levinud petuskeemi, mis eestlasi 2025. aastal Internetis kõige enam tabasid

10 kuud tagasi - 01.01.2026 Autor: AM

Lõppenud aasta on tõestanud, et petuskeemid ei piirdu enam lihtsalt e-kirjade ega kahtlaste sõnumitega. Nüüd on need targemad ja tihtilugu väga isiklikud. Ainuüksi Politsei- ja Piirivalveameti (PPA) esimese poolaasta statistikast selgub, et eestlased kaotasid petturitele ligi 7,6 miljonit eurot, millest üle 4,5 miljoni moodustasid telefonipettused.

Elisa infoturbejuht Mai Kraft hoiatab, et just inimlik usaldus, mõnetine naiivsus ja kiirustamine on see, millele petturid kõige enam panustavad: "Kui inimene tunneb, et peab reageerima kohe ja pikalt mõtlemata – olgu see siis panga, juhi või sõbra sõnum –, on pettur oma töö juba pooleldi ära teinud. See ei tähenda aga, et end ei saaks kaitsta. Tõeline kaitse algab sellest, et teame, millised pettused parasjagu liikvel on."

Kraft toob välja viis levinud petuskeemi, mille abil on tänavu Eesti inimestelt ja ettevõtetelt raha varastatud.

1. "Tere, olen sinu ettevõtte juht" – ärimeilide ja sõnumite võltsimine

Üks levinumaid petuskeeme seisneb selles, et ettevõtte töötajatele saadetakse juhi või partneri nime alt e-kiri või SMS, milles palutakse teha kiire ülekanne, soetada mõni digitaalne toode või jagada tundlikke andmeid. Petturid mängivad hierarhia ja usalduse peale, mistõttu inimene reageerib sageli ilma kontrollimata – kui "juht" kirjutab, et midagi on vaja, siis nii ka tehakse.

Kuidas end kaitsta?

- Kontrolli alati saatja e-posti aadressi või telefoninumbrit;
- kui sõnumis on kiireloomuline ja kahtlane palve, helista üle ning küsi, kas väidetav saatja on selle päriselt saatnud;
- ole eriti skeptiline, kui palved tulevad ebatavaliste kanalite kaudu, näiteks WhatsAppis.

2. Pakihoiatusega peibutamine

Petturid kasutavad massiliselt pakiteavituste võltsimist. Inimene saab SMS-i või e-kirja väidetavalt kullerfirmalt, kus palutakse maksta väike tasu või uuendada andmeid, et pakki ei saadetaks tagasi.

Link viib aga libalehele, mis varastab kasutaja andmed või kaardiinfo.

"Pakifirmadena esinevad pettused on tõhusad, kuna üha enam tellitakse kaupu internetist ja kes meist ei tahaks oma pakki võimalikult kiiresti kätte saada. Just sellele kiirustamisele petturid panustavadki," selgitas Kraft.

Kuidas end kaitsta?

- Ära ava linke tundmatutelt saatjatelt;
- kontrolli paki staatust otse teenusepakkuja ametlikul veebilehel;
- vaata hoolikalt üle saatja nimi ja number – ka väike erinevus võib olla oluline.

3. Kiire kasum "investeerimiskontol"

Libainvesteeringute skeemid lubavad kiiret ja kindlat tootlust. Petturid kasutavad sageli sotsiaalmeedias levivaid võltsreklaame, kus on kasutatud tuntud Eesti ettevõtjate või poliitikute pilte ja nimesid. Tavaliselt lubatakse ainulaadset investeerimisvõimalust ning juhendatakse samm-sammult konto loomiseni, mis suunab raha tegelikult petturi kontole.

„Mitte ükski edukas investor ei kutsu teisi üles kiirelt rikkaks saamise skeemiga liituma," märkis Kraft.

Kuidas end kaitsta?

- Kontrolli, kas investeerimisettevõte on Finantsinspektsiooni nimekirjas;
- kui pakkumine kõlab liiga hästi, et olla tõsi, siis see tõenäoliselt seda ka on;
- ära jaga oma isiklikke andmeid tundmatutel platvormidel.

4. Libarakendused ja pahavara telefonis

Üha enam levitatakse võltsrakendusi, mis jäljendavad panku, kullerfirmasid või investeerimisplatvorme. Rakenduse allalaadimisel ja õiguste andmisel saavad petturid ligipääsu seadmes olevatele andmetele.

Kuidas end kaitsta?

- Laadi rakendusi ainult ametlikest poodidest (Google Play, App Store);

- hoia seadme tarkvara ajakohasena;
- kui tööandja haldab nutiseadmeid, kasuta ettevõtte soovitatud turvameetmeid.

5. "Sõber" küsib raha

Sotsiaalmeedias levivad kontode kaaperdamised, mille puhul petturid saadavad tuttava nime alt sõnumeid stiilis „Kas saad mulle kiirelt raha laenata?“ või „Palun kinnita see kood“. Ohver usub, et suhtleb tuttavaga – kuni raha või andmed on kadunud.

„Sellised pettused mängivad inimlike emotsioonide ja kiirustamise peale,“ ütles Kraft.

Kuidas end kaitsta?

- Kui sõber küsib midagi ebatavalist, helista talle üle;
- ära jaga kunagi sisselogimiskoode ega kinnita Smart-ID või Mobiil-ID päringuid kellegi palvel.

Aeglane mõtlemine päästab

Krafti sõnul võivad abiks olla ka tehnilised lahendused, näiteks Elisa Netivalvuri teenus või viirusetõrje, kuid need ei asenda läbimõeldud ja teadlikku käitumist. "Kõige tõhusam kaitse pettuste vastu on teadlikkus, rahulik tegutsemine ja kaine mõistuse säilitamine. Enamik pettusi töötab ainult siis, kui inimene tegutseb läbimõtlematult," rõhutas ta.

- Uudised

- Lahendused
- Turvalisus

Pilt

