Mida saab teha, kui oled kurjategijad juba oma pangakontole sisse lasknud?

4 kuud tagasi - 29.12.2025 Autor: AM

Igasuguste Internetis levivate petuskeemide ohvrid annavad igapäevaselt kurjategijatele ligipääsu oma pangakontole ja õiguse nende nimel tehingute tegemiseks. Kui oled liiga hilja avastanud, et tegu on pettusega, kuidas siis käituda ning kuhu pöörduda, et kahju oleks võimalikult väike?

„Küberkurjategijad saadavad petukirju või teevad telefonikõnesid sageli kas tööpäeva lõppedes või hilisel ajal, sest inimene on siis väsinud või tüüdatakse teda hetkel, kui tal pole piisavalt aega mõelda küsitule ja tähelepanu hajub kergemini," hoiatab Telia küberturbe lahenduste arhitekt Matis Palm.

Sarnase juhtumiga puutus Palm hiljuti ka ise kokku, kui ühel Telia üritusel astus Telia küberturbe tiimi juurde mures mees, kelle tütar oli öösel saanud näiliselt ametliku kirja Tervisekassast, kust lubati raha tagastamist.

Neiu oli heauskselt sisestanud oma Smart-ID PIN-koodid ja helistanud siis isale, et küsida, miks Tervisekassa raha tagasi annab.

„Muutsime kiiresti neiu pangakonto limiidid miinimumi, vahetasime kasutajanime ja sulgesime Smart-ID," loetleb Palm tegevusi, mis tuli kiiresti ära teha, et juba kontole ligi pääsenud kurjategijate plaane takistada.

Pank kinnitas hiljem, et kontole oli korduvalt püütud sisse logida, kuid just kiire tegutsemine pani katsed seisma.

Palm selgitab, et pettuse ilmsiks tulekul ongi võtmesõnaks kiire tegutsemine. Kui oled kurjategijatele andnud ära oma PIN1, siis see tähendab, et oled andnud neile võimaluse oma kontodele sisse logida ja järgmiseid tegevusi planeerida ning sind psühholoogiliselt mõjutada kas erinevate kõnede, järjepidevuse või muul viisil, et sisestaksid nende nimel ka oma allkirja ehk PIN2-e.

Kui petturid on saanud kätte ka sinu PIN2 kinnituse, võivad nad ohvri nimel tehinguid kinnitada, uusi kiirlaenusid vormistada, ostu-müügitehinguid algatada ja luua ohvri nimel uue Smart-ID konto, mille puhul kaob vajadus sinu vanade PIN koodide jaoks.

Mida teha, kui oled sisestanud või kelmile öelnud oma PIN1-koodi?
(Sõltuvalt lahendusest, mida kasutad)

1. Tühista või sulge oma Smart-ID (seda on võimalik alati uuesti algatada ja luua).
2. Mobiil-ID puhul saab Mobiil-ID teenuse lõpetada või muuta Mobiil-ID PIN koodid (otsi telefonist rakendust Mobiil-ID). Mobiil ID saab lõpetada Telia esinduses (enne 02.07.2022 väljastatud Mobiil-ID) või iseteeninduses (alates 02.07.2022 väljastatud Mobiil-ID). Mobiil-ID teenus lõpetatakse ka siis kui kasutaja muudab Telia iseteeninduses kasutaja andmeid ja kustutab sealt isikukoodi.
3. Kui ID-kaardi PIN-koodid on lekkinud või kaart kadunud, tuleb sertifikaadid tühistada vastava juhendi järgi, mille leiad siit: https://www.id.ee/artikkel/id-kaardi-sertifikaatide-peatamine/.
4. Teavita oma panka ja palu kontrollida potentsiaalsete kahtlaste tegevuste või sisselogimiste kohta ja küsi nõu järgmisteks sammudeks.
5. Kontrolli, ega sinu nimel pole algatatud toiminguid (laenutaotlusi, uute teenuste avamisi).

Mida teha, kui oled sisestanud nii PIN1 kui ka PIN2?

1. Helista kohe oma panka – vajadusel blokeeritakse konto, kaardid ja internetimaksed.
2. Smart-ID koodide lekkimisel tühista vastavas iseteeninduspportaalis oma Smart-ID (või Mobiil-ID) viivitamatult.
3. Kontrolli oma pangakontosid ja elektroonilisi tehinguid.
4. Tee politseisse avaldus, kuna tegemist on kriminaalse pettusega. Kirjelda detailselt, kuhu sisestasid või mis kanalit pidi jagasid oma koodid ja kirjelda ka tegevused, mille oled ette võtnud peale andmete lekkimist.
5. Jälgi oma ID-identiteedi võimalikku väärkasutust e-teenustes ja lepingutes. Vajadusel teavita ka RIA-t või CERT-EE’d kui on kartust identiteedi ära kasutamise osas.

Palm tuletab meelde, et päris ametiasutused ei saada kunagi linke ega helista küsimusega, et jagada oma PIN koode: „Kui sõnum või kõnes küsitu tekitab kasvõi hetkeks kahtlust, tuleb see sulgeda ja suhelda ametiasutusega otse nende kodulehel olevate kontaktide kaudu.“

Eraldi teemaks on autentimine klienditeeninduse kaudu. Kui klient pöördub ise õige kanali kaudu (näiteks telekomioperaatori või panga IVR-süsteemi kaudu), tuvastatakse isikusamasus tavaliselt Mobiil-ID või Smart-ID PIN1 abil, et kinnitada

helistaja isik ja õigus saada või jagada lepingu- ning isikuandmeid. Sellegipoolest ei küsi klienditeenindaja kunagi PIN-koodi häälega välja ütlema ega e-kirjas edastama.

Samuti tuletab ta meelde, et pettuste ohvriks langevad inimesed vanusest, haridustasemest ja ametikohast sõltumata, sest kelmid muutuvad järjest nutikamaks, nende kirjad näevad iga kuuga professionaalsemad välja ning kõnede teostamiseks värvatakse puhast eesti keelt kõnelevaid isikuid.

„Kõige tähtsam on mõelda kaks korda enne tegutsemist ning rakendada lihtsaid, ent tõhusaid ettevaatusabinõusid. Soovitame kõigil hoida pangaülekannete limiidid igapäevaselt madalal tasemel – nii on võimalik kahju oluliselt väiksem," selgitab Palm.

Avafoto: nano Banana (Gemini) AI

- Uudised
- Turvalisus

Pilt