Kurjategijad võivad viipemakse mugavust kurjasti ära kasutada

4 kuud tagasi - 02.07.2026 Autor: AM

Viipemakse populaarsuse kasv on toonud kaasa uusi pettusviise, millega kurjategijad koguvad makseid ühistranspordis, turismipiirkondades ja QR-koodide kaudu.

Telia küberturbe lahenduste arhitekt Kristjan Aljas ütles, et kurjategijad teavad viipemaksete kasutuspiire ning kasutavad neid ära olukordades, kus makse läheb läbi ilma lisakinnitamiseta. Tema sõnul võimaldab isikliku makseterminaliga kurjategijal koguda makseid lihtsa vaevaga näiteks rahvast täis ühistranspordis.

Aljase sõnul on Eestis ja välismaal levinumaks muutunud lahendus, kus kurjategija kasutab mobiilset kaarditerminali ja võtab rahvarohkes kohas inimestelt makseid. Ohver ei pruugi märgata, et tema kaardilt on raha läinud, sest tehing näib hiljem pangaväljavõttel tavalise väikese ostuna.

Nuti- ja maksesõrmused sattuvad sihikule

Aljas tõi eraldi välja pettused, mis puudutavad nuti- ja maksesõrmuste omanikke, eriti puhkuse ajal. Kirjeldatud skeemis läheneb pettur turismipiirkonnas inimesele, pakub pildistamise abi ning kasutab telefoni makseterminalina, et sõrmusega makse vastu võtta.

Sellisel juhul ei pruugi inimene pettust märgata enne, kui konto väljavõttelt tehingud ilmnevad.

Turvameetmed aitavad kahju piirata

Swedbanki finantskuritegude ennetamise juht Eero Ergma ütles, et viipemakse on küll üks turvalisemaid makseviise, kuid riskide vähendamiseks tasub seada kaardile mõistlikud makselimiidid. Tema sõnul aitab see võimaliku pettuse korral kahju väiksemana hoida.

Ergma soovitas telefoni, nutikella või maksesõrmusega makstes eelistada digitaalseid rahakotte nagu Apple Pay, Google Pay või panga toetatud lahendused. Tema selgitusel lisavad need maksetele täiendava turvakihi, sest

kaupmehele ei jagata tegelikke kaardiandmeid.

Lisaks soovitas Ergma sisse lülitada mobiiliteavitused, jälgida regulaarselt pangakontot ning hoida pangakaarti ja nutiseadmeid turvalises kohas. Kui seadmel on võimalik maksefunktsioon ajutiselt välja lülitada, tasub seda teha olukordades, kus maksmist ei ole vaja või keskkond tundub ebaturvaline.

QR-koodide pettused sagenevad

Aljase sõnul suurenevad suve eel ka QR-koodi pettused. Laadal või suurüritusel võib pettur asendada õige QR-koodi enda omaga ning suunata kasutaja võltsitud veebilehele.

Aljas ja Ergma soovitasid suhtuda ettevaatusega kõikidesse QR-koodidesse, olgu need restoranis, tänaval või lennujaamas. Võltsitud koodi ei ole võimalik palja silmaga ehtsast eristada, mistõttu tuleb kontrollida, millisele veebiaadressile see suunab.

Kahtluse korral tuleb tegutseda kohe

Pettuseohule võivad viidata olukorrad, kus pärast koodi skaneerimist soovitatakse paigaldada tarkvara, küsitakse isiku- või krediitkaardiandmeid või nõutakse tuvastamist Mobiil-ID või Smart-ID abil. Sellisel juhul tuleks toiming katkestada.

Kui pettus on juba aset leidnud, soovitas Ergma kaart mobiiliäpis sulgeda või blokeerida, vajadusel esitada tehinguvaidlustus ning järgida panga juhiseid. Vajaduse korral tuleb pöörduda ka politseisse.

- Uudised
- Turvalisus

Pilt


VISA