Google tõttab Androidi kasutajatele appi tehisaru petukõnede vastu võideldes

2 tundi tagasi - 04.06.2026 Autor: AM

„Tere, ema siin!“ – aga mis siis, kui toru otsas on hoopis kurikaval tehisintellekt? Google tõttab Androidi kasutajatele appi ja toob välja oma tehisarutuvastaja, mis petukõned blokeerib.

Vaja läheb Androidi ja Phone by Google äppi, samas peab olema installitud ka Google Messages ja Google Contacts. Kui kahtlane tegelane (või masin) helistab, läheb helistaja poolt, kui ta kasutab ka Androidi, vastuvõtjale salajane kood. Tegemist on krüpteeritud "käepigistusega" teenusega RCS (*Rich Communication Services*).

Kõige usutavamad petuskeemid kuvavad vastuvõtja ekraanile mõne tuttava kontakti nime, näiteks ekraanile kuvatakse kiri „Ema“. Võtad kõne vastu ning kuuled tuttavat häält, täpselt sama kõlaga nagu alati. Kuid su väidetav ema on suures hädas ja palub kiiresti raha üle kanda. Sa ei kõhkleks, kuigi tegelikult peaksid küll. Tänapäeva küberkelmid suudavad internetitarkvara abil võltsida helistaja telefoninumbrit ning kasutada vabalt kättesaadavat tehisintellekti, et kopeerida lähedaste hääli nii täiuslikult, et inmkõrv ei suuda enam vahet teha. Enamasti kehtib see küll inglise keeles, kuid on muutunud juba väga kvaliteetseks ka väiksemates keeltes, sealhulgas eesti keeles.

See ulmefilmi meenutav stsenaarium on muutunud juba reaalsuseks ja toonud mujal maailmas kaasa sadu miljardeid dollareid kahju. Google on otsustanud sellele õudusele punkti panna, tuues sel kuul välja turvafunktsiooni nimega "*fake call detection*" (võltsitud kõnede tuvastamine).

Kuidas telefonid selja taga „salajast käepigistust“ teevad?

Selleks, et keerulist tehnoloogiat lihtsamalt mõista, võib uut funktsiooni kujutada kui kahe seadme vahelist salajast ja ülikiiret käepigistust.

Kui keegi sinu tuttavatest sulle helistab ja mõlemad kasutavad Google'i ametlikku helistamisrakendust, teevad telefonid taustal midagi sellist, mida me varem nägime vaid spioonifilmides.

Niipea kui kõne alustatakse, saadab helistaja telefon sinu telefonile reaalajas hääletu ja tugevalt krüpteeritud digitaalse kinnitussignaali. See on justkui salajane parool, mis tõestab, et kõne tuleb tõepoolest sellest konkreetsest seadmest. Kui aga sinu numbrile helistab pettur, kes on sinu tuttava numbri lihtsalt arvutiprogrammiga ekraanile mananud, jääb see digitaalne parool tulemata.

Google selgitab süsteemi toimimist järgmiselt:

> „Kui pettur üritab kontaktisikut teeselda, jääb see esialgne kinnitussignaal puudu. Kõne vastuvõtja seade märkab seda kohe ja saadab päringu kontakti tegelikule seadmele, et asja üle kontrollida.“

Kui sinu tuttava päris telefon vastab võrgus automaatselt: „Mina praegu ei helista,“ lööb sinu telefon kohe häirekella.

> „Kui nende päris seade vastab: „Mina praegu ei helista,“ kuvatakse teie ekraanile hoiatus, mis soovitab kõne kohe lõpetada. See ennetav hoiatus aitab reaalajas vältida süvavõltsingu ohvriks langemist ja telefoninumbri võltsimist,“ märgib Google.

Numbrinäit ei ole enam ammu usaldusväärne

Aastaid oleme harjunud pimesi usaldama seda nime või numbrit, mis telefoni ekraanile ilmub. Tänapäeval on see aga umbes sama turvaline kui uskuda tänaval võõra inimese rinnale kleebitud nimesilti.

Kurjategijad kasutavad ära asjaolu, et inimesed ei võta tundmatuid numbreid vastu, ning maskeerivad end tuttavateks, pankadeks või tööandjateks.

Probleemi ulatus on hiiglaslik. USA Föderaalne Kaubanduskomisjon (FTC) hoiatas, et ainuüksi 2024. aastal ulatusid petturite tekitatud kahjud miljarditeni, ning INTERPOL-i 2026. aasta märtsi finantspettuste aruanne märkis isikute impersoneerimist ühe peamise ohuna, mis viis eelmisel aastal maailmas enam kui 400 miljardi dollari suuruste kahjumiteni.

Google märgib otsekoheselt:

> „Aastaid on inimesed lootnud helistaja tuvastamisele (caller ID), et teada saada, kes on liini teises otsas, kuid petturite uute taktikate tõttu ei ole see enam piisav.“

Uus kaitsekilp on ehitatud avatud RCS-standardile (*Rich Communication Services*) ning Google loodab, et ka teised telefonitootjad ja rakenduste loojad võtavad selle tehnoloogia tulevikus kasutusele, et muuta mobiilside taas turvaliseks. Uuendus rullub globaalselt lahti Androidiga seadmetele juba sel kuul, jõudes esimesena Google Pixeli seadmetesse.

Video URL

Nagu iga uue tehnoloogiaga, on ka siin oma tugevused ja piirangud, mida tasub teada enne funktsiooni aktiveerimist (kuigi Google'i seadmetes on see sisse lülitatud vaikimisi).

PLUSSID

- Ennetav reaalajas kaitse: tuvastab ohu enne, kui jõuad petturile oma andmed või raha loovutada.
- Täielik privaatsus: kuna kontroll toimub otsast lõpuni krüpteeritud RCS-süsteemi kaudu, ei kuula keegi sinu kõnesid pealt.
- Automaatne toimimine: ei nõua kasutajalt tehnilisi teadmisi ega pidevat seadistamist.
- Avatud standard: tehnoloogia on kättesaadav ka teistele tootjatele.

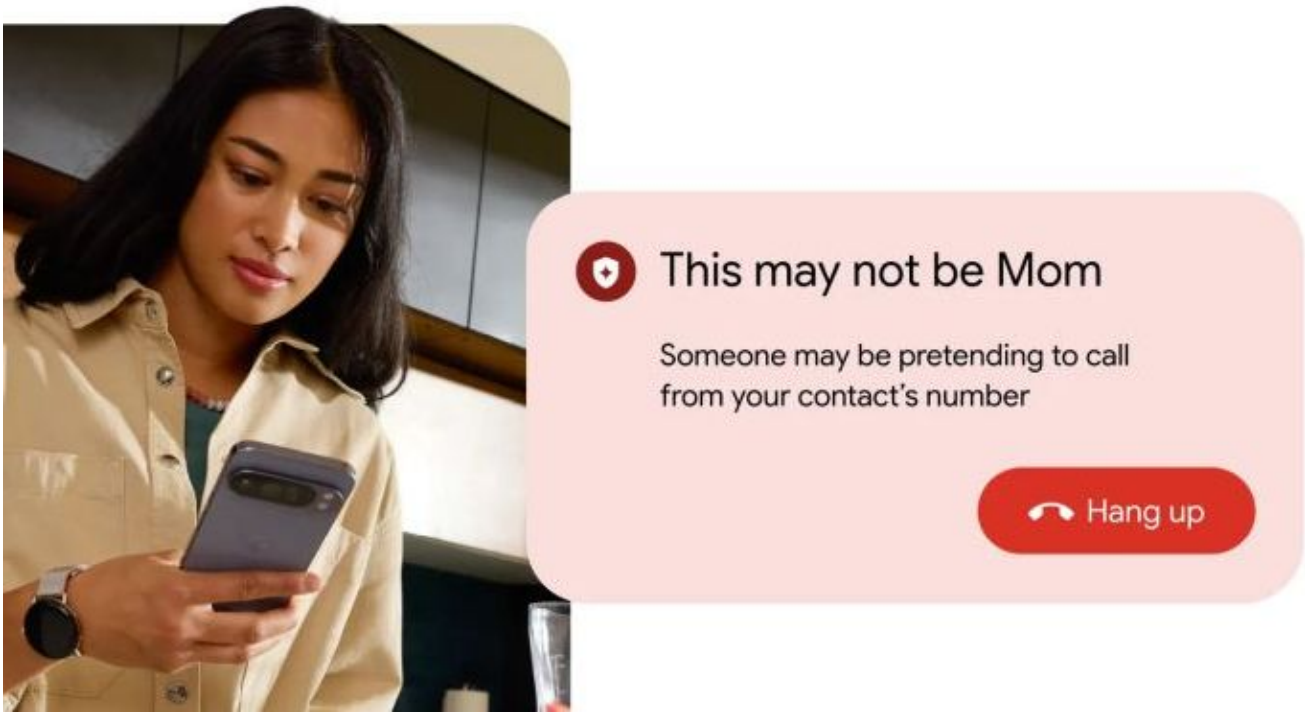
MIINUSED

- Piiratud ökosüsteem: toimib vaid siis, kui mõlemad osapooled kasutavad Androidi ja spetsiaalset Google'i helistamisrakendust.
- Sõltuvus internetiühendusest ja RCS-ist: vajab toimimiseks aktiivset andmesidet ja sisselülitatud RCS-funktsiooni sõnumirakenduses.

- Uudised

- Mobiiltelefonid
- Turvalisus

Pilt


This may not be Mom
Someone may be pretending to call from your contact's number
Hang up