Ekspert: e-kirjadele vastamine kohvikus või konverentsil ei olegi nii turvaline kui arvatakse

3 kuud tagasi - 30.01.2026 Autor: AM

Inimesed kasutavad igapäevaselt oma telefoni ning arvutit avalikes kohtades nagu bussis, kohvikus, rongis või trennis. Kuigi see tundub pealtnäha süütu tegevus, võib ekraanilt nähtav info olla midagi, mida hiljem saab kasutaja vastu kurjalt ära kasutada.

Turvateadlikkuse platvormi Phisbite tootejuht Urmo Keskel rõhutab, et oma isiklike meilide, kontode ja sõnumite kuvamine avalikus kohas on reaalne ohutegur ning iga tehnoloogia kasutaja peaks oma ekraani võõraste silmade eest kaitsma.

Oht ei ole vaid ühistranspordis või avalikes ruumides

Keskeli sõnul võivad pahatahtlikud silmad saada infot ka näiteks konverentsilt.

“Just hiljuti juhtus minuga olukord, kus kahe rea tagant nägin kellegi arvuti ekraanil infot valitsusasutuse juriidiliste probleemide kohta ja nägin meilivahetust tarnijast, kes tegi kehva tööd. Lisaks isiklikke kirju ja e-teenuste statistikat,” meenutab Keskel ja lisab: “Kui keegi sellises olukorras sisestab parooli, eriti ilma kahefaktorilise autentimiseta, võivad tagajärjed olla väga tõsised.”

Urmo Keskel.

Kõige levinum on viga, et ei arvestata infoga, mis on ekraanil, võivad avalikus ruumis võõrad näha ja salvestada. “Tänapäeva telefonide kaamerad on nii head, et päris kaugelt tehtud pildi puhul on võimalik näha, mis on teise kasutaja ekraanil ning mida sisestatakse,” selgitab ta, et kui kohvikus istuda akna all, võib tundlikku infot näha ja salvestada isegi juhuslik möödakäija.

Eksperdi sõnul on olukord, kus kõrvalistuja suudab varastada andmeid lihtsalt ekraani vaadates,reaalne vaid ühel juhul: “See risk on reaalne ainult siis, kui sotsiaalmeedia kontole sisenetakse sisestades käsitsi parooli ja mitte kasutades kahefaktorilist autentimist. Sel juhul võib pahatahtlik toimingu pealtnägija filmida parooli sisestamist ning pärast kasutada saadud paroole kontole pääsemiseks.”

Pangakonto puhul on oht väiksem. “Jällegi võib pahatahlik inimene näha teie panga kasutajatunnust ja ka isikukoodi ning pärast proovida teile saata autentimispäringu kasutades Smart-IDd või Mobiil-IDd,” selgitab Keskel ja toonitab, et sellise rünnaku puhul on oluline, et kui kasutajale hüppab telefonis ette Smart-ID või Mobiil-ID PIN sisestuse aken, siis mitte mingil juhul ei tohi seda toimingut kinnitada ja koode sisestada, kui pole ise toimingut algatanud.

Mis aitaks?

Keskeli sõnul saab riske maandada udutatud klaasiga. “Sellised lahendused aitavad oluliselt ekraanilt kuvatavate andmete lekkimise riski maandada. Eriti just

avalikus ruumis telefoni kasutamisel. Samas ka nende lahenduste puhul peab silmas pidama, et kui keegi on otse teie selja taga, siis ta võib ikkagi näha, mis teie ekraanil toimub," räägib ta.

Tihti muudavad telefoniekraanide kaitse- ning pimendamiskiled vaadatavuse ka omanikule uduseks. Õnneks areneb tehnoloogia aina kasutajasõbralikumaks ning turvalisemaks. Tehnoloogiahiid Samsung teatas hiljuti, et tuleb peagi välja uue privaatsuse funktsiooniga, mis pimendab ekraani nii kavalalt, et kasutaja ise näeb oma telefoni ekraani selgelt, aga kõrvalolijale on pilt täielikult pime. Firma sõnul on nad funktsiooni arendanud viis aastat ning see annab kasutajale võimaluse ise otsustada, millal ja kus ekraani sisu pimedaks teha või teavitusi kõrvalolijate eest peita.

Alari Pennar.

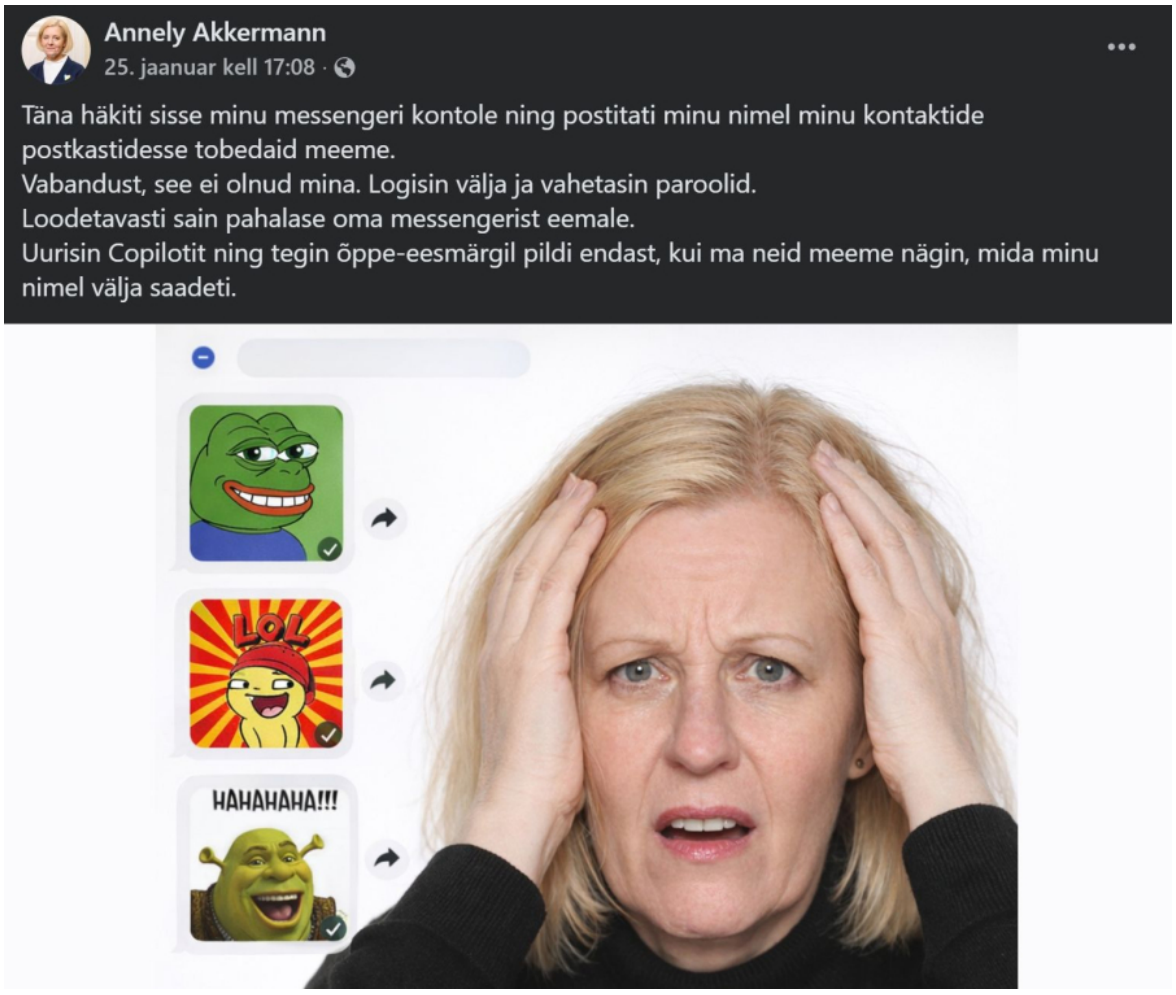
"Meie funktsiooni peamine eesmärk on teha seda, mida teised saavad osaliselt teha vaid füüsilise privaatsuse kilega," sõnab Samsungi koolitusjuht Alari Pennar ja lisab: "Funktsioon teeb ekraani tumedaks, justkui oleks ekraan välja lülitatud."

"Samsung on uurinud, kuidas inimesed telefone kasutavad ja ehitanud sellele toetuvalt lahenduse, mis töötab nii tarkvaras kui ka riistvaras. Arvestades kasutajaga, et funktsioon oleks turvaline, aga ei segaks igapäevast kasutamist," selgitab Pennar.

Kuidas sa mu kontole said?

Sellest ei räägita palju, mis viisil on kellegi kontole ja isikuandmetele ligipääs saadud. Just hiljuti kajastas meedia juhtumit, kus riigikogu liikme Annely Akkermanni Facebooki konto võeti üle ning sellelt saadeti tema nimel sõnumeid. Annely ei osanud täpselt öelda, kuidas tema kontole ligi pääseti.

“Kõrvalt piilumise ja koodide salvestamise juhtumid on teemaks pigem lähedaste ringis, kus üks pereliige (nt. laps) püüab salaja teise pereliikme telefonile või sotsiaalmeedia kontodele ligi saada,” selgitab Keskel ja toonitab, et sageli kasutajad ei adu, milliseid telefonis olevaid andmeid nende rakendused töötlevad ning millistesse pilveteenustesse ja suurtesse tehisintellekti mudelitesse inimeste andmed töötlemiseks liiguvad.



Ekraanipilt Facebookist.

“Üldine soovitus on, et avalikus ruumis telefoni ja teiste nutiseadmete kasutamisel tuleks eeldada, et keegi võõras võib ekraanil olevat näha ja salvestada nii, et ise ei pane seda tähelegi. Ka telefoni- või videokõnede puhul tasub mõleda, et kui tundlik on räägitav info ja mis juhtub kui sellest lähedal

olevad inimesed kuuleva,” soovitab Keskel.

“Kui avalikus ruumis on vaja ekraani vaadata, siis pigem teha seda nii et telefon on madalamal (nt. süles). Kui tõesti on konverentsil vaja arvuti ekraani kasutada ja sealt midagi tundlikku vaadata, siis teha seda viimases reas, kus kedagi ei ole selja taga. Kõrvalistujate osas aitab ekraanifiltri kasutamine,” lisab ta, et inimesed peaksid kindlasti kasutama ekraanilukku. Kui telefon kaob, ei saa võõras selle sisu näha. Kasutama kahefaktorilist autentimist, sest see lisab paroolile täiendava turvakihi.

- Lahendused
- Turvalisus

Pilt