Kavalad nipid, millega inimene avalikus ruumis pettuselõksu meelitatakse

6 kuud tagasi - 23.05.2026 Autor: AM

Kes poleks vahetevahel ühendanud arvutit mõnda tasuta WiFi-võrku, kohvikumenüü vaatamiseks skaneerinud QR-koodi või laadinud mobiili akut avalikus laadimispunktis? Kõik need pealtnäha süütud tegevused võivad inimesele lõppeda tühjaks tehtud pangakonto või tema tööandjale tekitatud massilise andmelekkega. Millised on kuus enamlevinud lõksu, mis avalikus ruumis varitsevad ja kuidas neid vältida?

„Avalikus ruumis tasub olla ettevaatlik, sest kurjategijad kasutavad ära inimese heausksust. Eriti aktiivseks muutuvad avaliku ruumi pettused suve eel kui inimesed liiguvad rohkem ringi ning üritavad sageli sobitada puhkamist kaugtöötamisega," hoiatab Telia küberturbe lahenduste arhitekt Kristjan Aljas.



Kristjan Aljas.

Tema sõnul loodavad kurjategijad avaliku ruumi paigutatud lõksude abil kätte saada nii inimese raha, aga ka näiteks ligipääsu tema tööandja andmebaasidele, et sealtkaudu teenida palju suuremaid summasid. Seetõttu peaks tööandja kehtestama kindlad reeglid kaugtööle ja seadmete kasutamisele. Näiteks peaks

olema kindlasti kasutusel VPN ehk niinimetatud virtuaalne privaatvõrk, mis võimaldab kaugtööd teha turvaliselt, luues seadme ja interneti vahel krüpteeritud tunneli, mis kaitseb andmeid ja varjab IP-aadressi.

„Kuigi kaugtöö on laialt levinud, eriti suvel, siis VPN-i kasutamine on jätkuvalt paljudele võõras. Näiteks Kantar Emori ja Telia koostöös valminud IT-turvalisuse uuringust tuli välja, et see on kasutusel vaid poolel Eesti ettevõtteist," räägib Aljas.

Sarnaselt VPN-i kasutamisega peaks töötajas olema juurutatud arusaam, et seadmete operatsioonisüsteemid ja rakendused peavad olema uuendatud, sest see välistab väga levinud ründetüübi ehk võimaluse siseneda tarkvara turvaaugu kaudu. Samuti tuleb veenduda, et n-ö back-up on alati korras ehk kui arvuti läheb katki, varastatakse või nakatub, on võimalik andmed sellegipoolest taastada.

Üks suuremaid ja samas enam alahinnatud ohuallikaid on avalik WiFi-võrk. Näiteks luuakse hotellifuajeesse, kohvikusse või lennujaama libavõrk, mil nimeks näiteks „FreeWiFi" või mõne tuntud sideoperaatori nimi.

„Kui ühendad tulemüürita ja VPN-ita ja uuendamata tarkvaraga seadme võõrasse võrku, on kõik paroolid, failid ja tegevused ründajale näha. Halvimal juhul saab ründaja arvutile või telefonile kaugligipääsu ja muudab selle nn botiks, mis levitab pahavara ja krüpteerib faile," hoiatab Aljas.

Levinud on ka võlts-QR-koodid, mis näiteks restoranis suunab inimesi paigaldama peturakendust, lubades selle eest 50% allahindlust. Sellise QR-koodi võib leida ka rahvarohkelt ürituselt või näiteks lennujaamast, kus suvalise posti külge kinnitatud QR-koodi skaneerijale lubatakse näiteks paigutamist turistiklassist äriklassi. „Tegelikult seda loomulikult ei saa, aga lennu ajal võidakse teha tühjaks ohvri pangakonto või varastada seadmest tundlikke andmeid," kutsub Aljas suhtuma QR-koodidesse ettevaatusega. Ta lisab, et eriti ettevaatlikuks peaksid tegema juhtumid, kus QR-skaneerimisel küsitakse isikuandmeid või palutakse end tuvastada näiteks Mobiil-ID või Smart-ID kaudu.

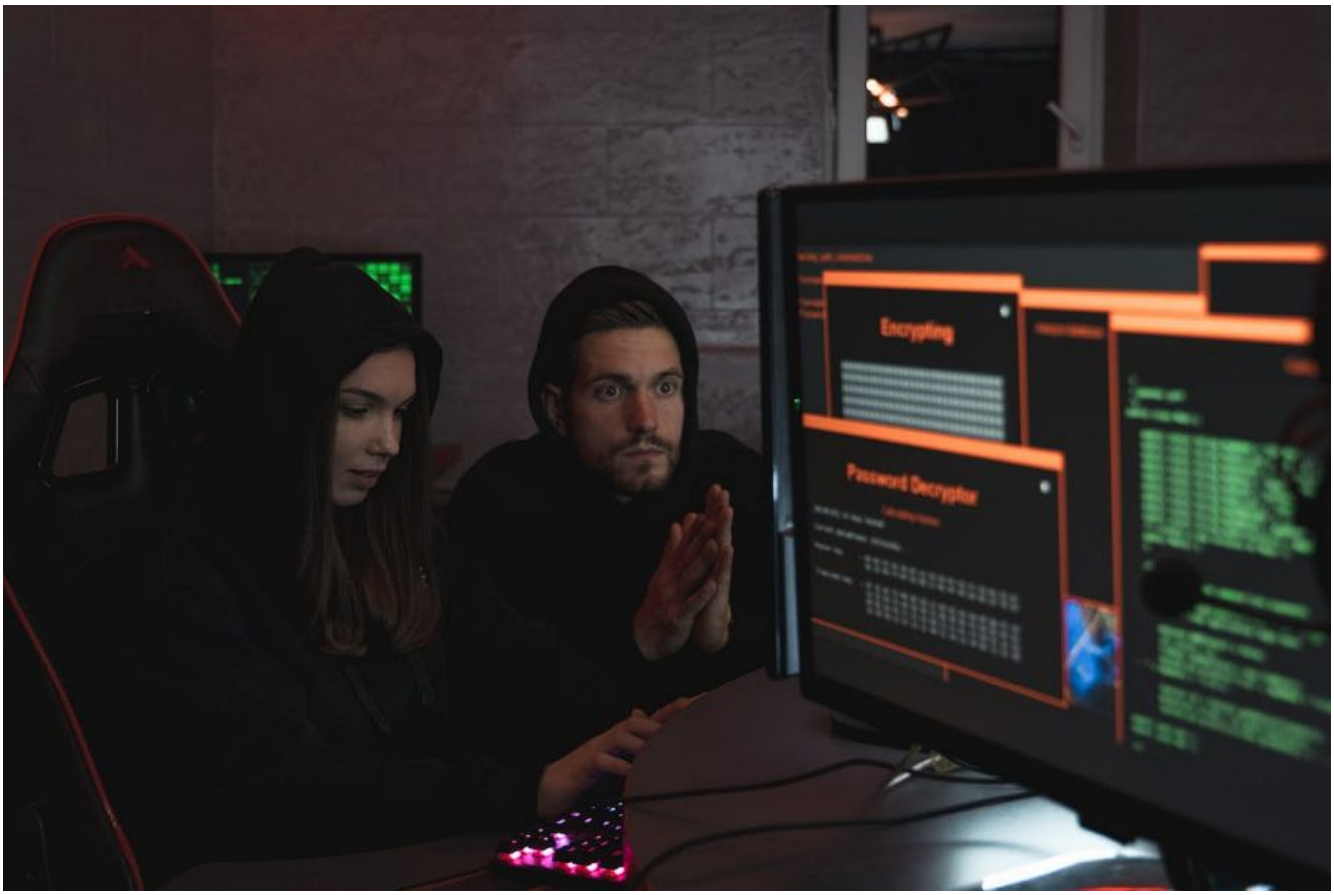
Sarnane oht peitub ka avaliku telefonilaaduri USB-pesas. Aljase sõnul kasutavad kurjategijad kaableid, mis suudavad telefoni andmed alla laadida kasutajalt luba küsimata. „Mobiilil on aku tühi ja see ühendatakse esimesse vabasse pistikusse, mõtlemata, et see võib teha enamat kui telefoni laadida," nendib ta.

Ettevaatlik tasub olla ka avaliku ruumi kaameratega. Aljase sõnul juhtub järjest sagedamini, et „turvakaamera" salvestab hoopis ohvri ekraanipilte ehk näiteks arvutisse sisestatud paroole ning info jõuab lõpuks kurjategijateni.

Kui tahad reisil kaugtööd teha, siis:

1. Mõtle läbi, kas tööseade on ikka vaja kaasa võtta. Kui ei, jäta see koju. Vähem seadmeid reisil tähendab vähem riske.
2. Kontrolli, et seadme tarkvara oleks alati uuendatud. Paikamata turvaauk on ründaja peamine sissepääs. Veendu, et nii operatsioonisüsteem kui ka rakendused on alati ajakohased.
3. Kasuta alati VPN-i. VPN krüpteerib kogu liikluse ja peidab sinu tegevuse võõras võrgus.
4. Lülita sisse kaheastmeline autentimine. Isegi kui parool lekib, kaitseb teine autentimiskiht sinu kontosid.
5. Kustuta kasutamata äpid ja kontrolli varukoopiat. Vanad rakendused on turvarisk. Varukoopia peab toimima, et andmed oleksid kättesaadavad ka siis, kui seade kaob.
6. Ära skänni võõrast QR-koodi ega ühenda seadet tundmatusse laadimispessa. Kasuta oma laadijat ja suhtu kriitiliselt igasse linki, kuhu sind suunatakse.

Pilt


Encrypting
Password Decryptor