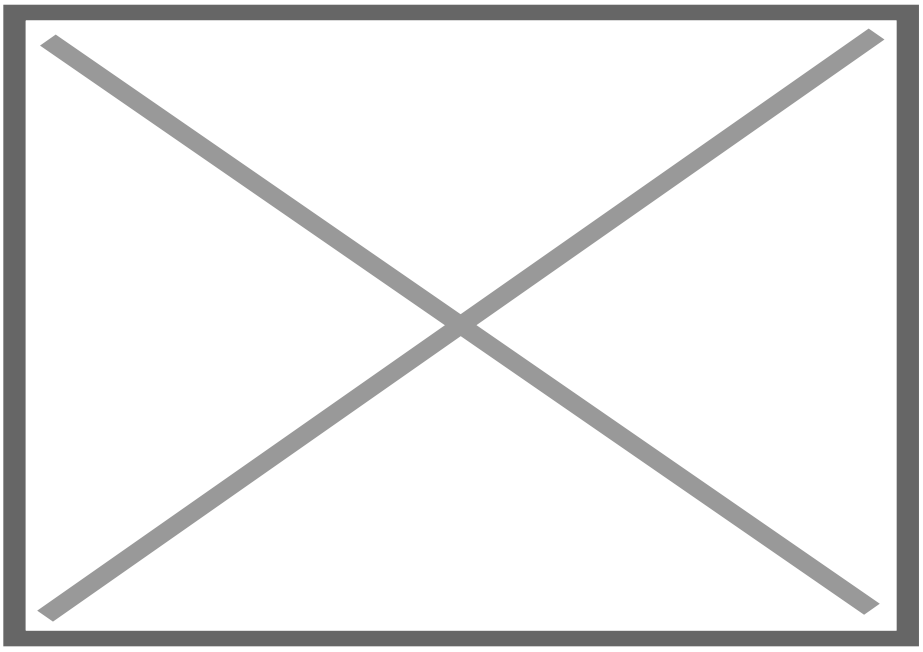
Mikrofonisegajad, kõnekrüpteerijad - kui kardad, hangi oma telefonile turvalisuse kest

11 aastat tagasi - 16.09.2015 Autor: AM



Nuhkimisjutud ja krimiseriaalid on närvi ajanud need, kellel on infot, mida varjata - kas küberkurjategijate või lausa valitsuste eest. Ärimehed, poliitikud, luurajad ning paranoilised kodanikud teavad, et Google, Microsoft, Apple ja kes kõik veel võivad alati nende infole nutitelefonis ligi pääseda, et parandada teenust ja tarkvara kvaliteeti. Kui vanal nuputelefonide ajastul said ärimehed kokku ja eemaldasid telefonidelt akud, enne kui sensitiivset juttu ajama hakkasid, siis nüüd pole paljudel see enam võimalik - aku on ju sisse ehitatud. Mida siis teha, et kaasavõetud telefoni mikrofoni kaudu salakõrv ei kuuleks ja nii esi- kui tagaküljel asuva kaamera kaudu salasilm ei näeks?

Vysk - segab mikrofoni, krüpteerib kõnesid, peidab kaamerad



Aitavad spetsiaalsed turvakestad telefonidele. Vysk´i mobiilikestad sobivad Apple´i ja Samsungi toodetele. Robustsevõitu, otsekui odavast 3D printerist tulevad telefonikuued on oma petlikule välimusele vaatamata üsna võimekad. Vysk krüpteerib kõik väljuvad kõned ja tekstisõnumid, segab mikrofoni või lülitab selle välja ja ning on varustatud luukidega, mis füüsiliselt käivad objektiivi ette - lihtne, aga efektiivne turvalahendus. Vysk EP1 on igapäevase tavakasutaja turvalisuse tagamiseks ja maksab 130 dollarit (värvivalik kuldne, sinine ja must,

hall) ning ettevõtte versioon QS1 maksab 230 dollarit.

EP1 on varustatud luukidega kaamerate sulgemiseks, QS1 segab lisaks ka mikrofoni, mis on telefoni sisse ehitatud.

Nii Androidile kui IOS-ile on tasuta rakendused Vysk Private Messaging ja Vysk Gallery, mis tagavad krüpteeritud sõnumside ja piltide turvalise salvestamine krüpteeritud pilveteenusesse.

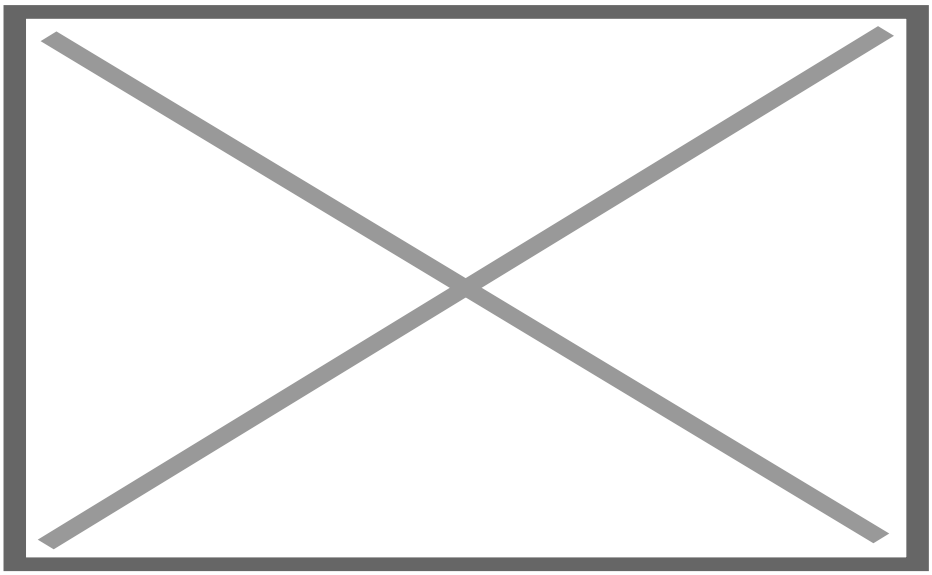
Äriettevõtted saavad hakata kümnedollarise kuutasuga krüptokõnede teenuse kliendiks, millega saadetakse üle Interneti kõned turvalisse serverisse ja neid pole võimalik pealt kuulata ka operaatori juures.

Kestad sisaldavad oma akut, mis annab iPhone´ile või Samsng Galaxyle vajadusel ka lisa-aega rääkimiseks. Kestad kinnituvad nagu tulnukaparasiidid telefoni tagaküljele, hõivates ka telefoni toitepesa. Akut saab nii kestal kui mobiilil laadida kesta enda microUSB pistikust.

Mobiilikatted ei salvesta kõneajalugu - eks see teeb kasutamise natuke ebamugavaks, kuid samas pole ka kõnelogisid, mida saaks hiljem uurida.

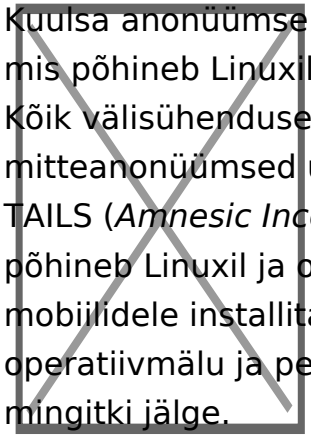
Osta terve telefon, mis on turvaline

Kui tahad aga õhukest ja normaalse välimusega telefoni, siis ülalolev robustne kest pole ilmselt sobiv. Ära tuleb oodata Blackphone 2, mida saab juba eeltellida ja mis septembri jooksul peaks välja tulema. Selle riistvara ja tarkara on tootja - Silent Circle´i - sõnul puhastatud võimalikest nuhkijatest ja midagi ei saadeta kellelegi kolmandale. Silent Circle'i SilentOS on Androidi lähtekoodist kokku pandud uus turvaline operatsioonisüsteemi platvorm. Lisaks on kaasas hulk krüpteeritud side äpp´e.



Blackphone´i oluline puudus on äriettevõtetes see, et tänapäeval ei taha enam keegi korporatiivset telefoni, vaid ikka enda oma kasutada ka tööl ning nõuda selle eest hüvitist. Nii kadus Blackberry turult, sest tööinimesed hakkasid korporatiiv-asju ajama oma eratelefonidega. Nii võib isegi Vysk´i kestal rohkem tulevikku olla: ole siis tööl oma iPhone´iga, aga tõmba 9-17 ajal see turvakest ümber!

Tõmba Android, mis ei jäta mingeid jälgi



Kuulsa anonüümse võrgu TOR loojad on valmis teinud ka operatsioonisüsteemi, mis põhineb Linuxil ja mis ei jäta kasutajast maha mitte mingeid digitaalseid jälgi. Kõik välisühendused käivad TOR´i anonüümse võrgustiku kaudu ja kõik mitteanonüümsed ühendusd blokeeritakse. Tegemist on operatsioonisüsteemiga TAILS (*Amnesic Incognito Live System* ehk unustav ja anonüümne süsteem), mis põhineb Linuxil ja oli algselt mõeldud PC-dele, kuid TOR on välja töötanud ka mobiilidele installitava rakenduse nimega Orbot. See kasutab vaid telefoni operatiivmälu ja peale sessiooni lõppu kustutab sealt kõik, jätmata kasutajast mingitki jälge.

Guardian ROM on samuti Android, mille arendamine käib XDA foorumis. Avatud lähtekood tagab, et midagi nuhkima kuhugi sokutada ei õnnestu. paranoilisemad kompileerivad koodi oma telefoni jaoks ise, olles selle vastavalt oma viitsimise ja oskuste tasemele enne üle vaadanud.

Muidugi ei pruugi sellise Androidiga kõik vajalikud äpp´id töötada ja kas on vajagi, sest paljud neist lekitavad andmeid...

Otsida võib veel ka DarkMatter´i nimelist Androidi ROM-i, mis on planeeritud töötama Samsung Galaxy ja Google Nexuse telefonidel. Viimasel ajal pole aga

sellest enam väga palju kuulda olnud.

Muud kasulikud abivahendid: pipragaas, röökiv telefon jne

Mõnikord aitab turvalisuse tagamiseks ka vähesest - näiteks see telefonikest Coyote Case käitub alarmina, kui kasutaja selle röövi ajal aktiveerib ning saadab ka hädakutsungi ettemääratud numbritele.

The Defender Case aga sisaldab.. ehtsat pipragaasi. Lisaks saadab alarmi ettenähtud numbritele ja mobiilikestaga saab salvestada ka huvitavaid pilte - nimelt sisaldab lisavarustus kaamerat, mis pildistab pipragaasisutsaka saanud kallaletungijat, et seda pilti saaks hiljem rünnaku tõestamiseks kasutada. Vaata videot tõhusast abivahendist:

- Uudised
- Turvalisus