

Yaliyomo:

[Utangulizi wa Jinsi ya Kuweka Kumbukumbu Wakati Mtandao Umezimwa](#)
[Kuseti Simu kwa Ajili ya Kuweka Nyaraka Wakati Hakuna Mtandao](#)
[Naweza Kutumia Aplikesheni hii ya Kuweka Nyaraka?](#)
[Kudumisha Taarifa Zinazoweza Kuthibitika Wakati Mtandao Umezimwa](#)
[Kuweka Chelezo Taarifa Zilizo Kwenye Simu Bila Mtandao au Kompyuta](#)
[Kusambaziana Faili na Kuwasiliana Wakati Mtandao Umezimwa](#) .

Utangulizi wa Jinsi ya Kuweka Kumbukumbu Wakati Mtandao Umezimwa Jinsi

Mwezi Juni 2019, ukiukaji wa haki za binadamu na migogoro ya kibinadamu, ilikuwa ikiendelea , nchini Myanmar, ambapo Wizara ya Uchukuzi na Mawasiliano nchini humo [iliagiza kampuni za mawasiliano](#) kuzima huduma za mitandao ya simu katika baadhi ya maeneo ya Jimbo la Rakhine na Jimbo la Chin. Akitaja “kuvurugika kwa amani” na “shughuli haramu,” serikali ya Myanmar ilidai kuwa ilitunga sheria hiyo ya kuzima mitandao “[kwa manufaa ya watu](#).” Kiuhalisia, kuzimwa huko kulizuia [zaidi ya watu milioni moja](#) kupata taarifa muhimu na kuwasiliana, na kuvuruga juhudi za misaada ya kibinadamu. Kama Matthew Smith kutoka [Fortify Rights](#), [alivyosema](#), “Kuzimwa huku kuna tokana na mauaji ya halaiki yanayo endelea dhidi ya Rohingya na uhalifu wa kivita dhidi ya Rakhine, na hata kama ililenga wapiganaji, yalikuwa makubwa sana kupita kiasi.”

Kuzimwa huko [kuli ondolewa kiasi tu katika baadhi ya miji mitano](#) mnamo Septemba 2019, japokuwa ni endelevu. Katika mwezi huo huo katika mji jirani wa Bangladesh, ambapo watu wengi wa Rohingya wame kimbilia, mamlaka ziliamrisha kampuni za simu [kufunga huduma za 3G na 4G](#) katika kambi za wakimbizi za Rohingya na kusimamisha uuzaji wa kadi za simu kwa watu wa Rohingya. Tulipo ingia mwaka 2020, [miji minne ya Rakhine](#) iliendelea kushindwa kuunganishwa na ulimwengu, na Bangladesh [iliendelea kuzuia huduma](#) katika kambi za wakimbizi.

Kuweka Kumbukumbu Wakati Mtandao Umezimwa

Ulimwenguni, kuzimwa kwa mtandao kunazidi kunaongezeka. Kulingana na kampeni ya AccessNow ya [\(#KeepItOn campaign\)](#) kulikuwa na visa 128 vya kuzimwa mitandao kwa makusudi kati ya Januari - Julai 2019, kulinganisha na 196 kwa mwaka mzima wa 2018, na 106 katika mwaka 2017, na 75 katika mwaka 2016. Kote ulimwenguni, serikali, kwa kushirikiana na makampuni ya mawasiliano ya simu, zimekuwa zikizima mitandao kama njia ya kukandamiza

jamii, kuzuia uhamasishaji, na kuzuia taarifa za ukiukwaji wa haki za kibinadamu kurekodiwa na kusambazwa.

“Kuzima mitandao na ukiukwaji wa haki za binadamu vina uhusiano wa karibu.”

- Berhan Taye, AccessNow

Kuzimwa kwa mitandao kunaweza kuwa na sura tofauti tofauti, ikiwemo [kufunga mifumo fulani ambayo inalenga aplikesheni na tovuti maarufu](#), [kuzima mitandao ya simu](#), [kudhibiti kasi ya mtandao](#), au [kuzima mitandao kabisa](#). Aina zote hizi za uzimaji mitandao zinalenga kuvuruga uwezo wa kuwasilisha taarifa na kuanika dhuluma na ukiukwaji kwa wakati huo huo unapotokea. Mara nyingi haya hutokea wakati wa maandamano, uchaguzi, na nyakati za migogoro ya kisiasa, na mara nyingi huandamana na ukandamizaji kutoka serikalini, mashambulizi ya kijeshi, na vurugu. Japokuwa serikali zinajaribu kutetea uzimaji mitandao kama [kisingizio cha “usalama wa umma” au sababu nyinginezo](#), hakika kuzimwa huku hutokea wakati serikali kandamizi ikihofia kupoteza nafasi ya kudhibiti watu wake, taarifa, au masuala ya kisiasa. Uzimaji hukiuka haki za binadamu, huvuruga [maisha na riziki za watu](#), na pia huwa na [athari za kiuchumi kwa dunia](#).

Kuweka kumbukumbu za ukiukwaji wa haki za binadamu ni muhimu kama ilivyo kawaida hata wakati mtandao umezimwa. Hata kama taarifa hazita sambazwa muda huo, kuchukua kumbukumbu kutakuwa njia ya kuhifadhi zile sauti ambazo mamlaka zinataka kunyamazisha, na kuweka ushahidi wa dhuluma ambazo zitakuja kutumika kama kidhibiti baadaye katika kuwawajibisha. Hata hivyo, ukandamizwaji na vikwazo vya kiteknolojia vya kuzimwa kwa mtandao hufanya kuchukua kumbukumbu za ukiukwaji na utunzaji wake kiusalama kuwa na changamoto na hatari. **Wanaharakati watawezaje kunasa na kuhifadhi video zao wakati mtandao umezimwa, na hata kusambaziana video hizo bila mtandao, na kufanya hivyo kwa njia salama?**

Mfululizo Huu

Kupitia kazi zetu na wanaharakati ambao wana uzoefu na uzimwaji mtandao, tumejifunza vitu muhimu na jinsi ya **kunasa na kuhifadhi kumbukumbu za video wakati mtandao umezimwa** ambao tuta shirikishana kwenye mfululizo huu. Tuliandika kwa kuangazia vifaa vya Android zaidi, japokuwa vitu hivyo vinaweza kutumika kwenye iPhones pia. Mikakati baadhi inahitaji maandalizi ya mapema (na mara nyingi, kuwa na mtandao), hivyo basi ni wazo zuri kuhakiki na kutekeleza hatua zozote zile *kabla* ya kujikuta katika mazingira ambayo hauna mtandao na unataka kuchukua kumbukumbu. Weka nakala mojawapo ya mafundisho ambapo utapitia au kusambaza wakati mtandao umezimwa. Na mwisho, anza kufanyia mazoezi mbinu na njia hizi katika shughuli zako za kila siku ili ziwe sehemu ya pili ya kawaida ya maisha yako kabla hujapitia katika hali mgogoro.

- Tayarisha
 - [Kuseti simu kwa ajili ya kuweka nyaraka wakati hakuna mtandao](#)
- Nasa
 - [Napaswa kutumia aplikesheni hii ya kuweka nyaraka?](#)
- Kuimarisha
 - [Kuimarisha taarifa zinazoweza kuthibitika wakati mtandao ukiwa umezimwa](#)
 - [Kuweka chelezo taarifa za kwenye simu katika sehemu nyingine bila kuwa na mtandao au kompyuta](#)
- Kusambaziana na Kuwasiliana
 - [Kusambaziana faili na kuwasiliana wakati mtandao umezimwa](#)

Maelezo ya mwisho: Wakati vidokezo hivi vikiendelea kukusaidia kuweka nyaraka wakati mtandao ukiwa umezimwa, tungependa kusisitiza kuwa suluhisho la mwisho ni kurudisha mtandao, na kupigania kwa ushindi [haki ya watu ya kurekodi](#), na uhuru wa kujieleza, taarifa, na kukusanyika. Kwa bahati mbaya, kuna harakati za kimataifa zikiongozwa na mashirika kama [NetBlocks](#), [AccessNow](#), na mengine mengi ambayo yanafuatilia kikamilifu na kupeana taarifa kuhusiana na uzimaji mitandao. Mawakili kote ulimwenguni wanaweka yao [mikakati ya madai ya kisheria dhidi ya uzimaji mtandao](#). Tunawaunga mkono kwenye kazi ya kutetea haki za binadamu.

Kuseti Simu kwa Ajili ya Kuweka Nyaraka Wakati Hakuna Mtandao

Makala hii ni sehemu ya mfululizo wa [Kuweka Nyaraka Wakati Hakuna Mtandao](#)

Imehakikiwa mwisho: 31 Januari 2020

Licha ya kuzimwa kwa mtandao, wachukua nyaraka bado wanaweza kunasa ushahidi muhimu wa video unaoweza kusambazwa bila kuwa na mtandao au watakapo pata mtandao.

Hivi hapa ni baadhi ya vidokezo ambavyo tumejifunza kutoka kwa wanaharakati na watendaji wengine kuhusu jinsi ya kuseti simu kuchukua nyaraka wakati hakuna mtandao. Kumbuka kuwa baadhi ya hatua **zitahtaji uwe na mtandao**, hivyo lazima zifanyike kabla mtandao haujazimwa au wakati mtandao utakapo rudi. Pia, usisubiri hadi uwe katika hali ya taharuki ndio uzingatie hatua hizi; zifanye sasa, na tafuta muda **ufanye mazoezi ya kutumia simu** kabla ya kuhitaji kutumia wakati wa migogoro.

Kuzimwa kwa mitandao mara nyingi hugongana na wakati taarifa zinadhhibitiwa na vikwazo vya uhuru kwa kujieleza na kukusanyika vikiwekwa. Kama wewe ni mchukua taarifa, jitahidi kuchukua tahadhari kujilinda mwenyewe na taarifa zako katika vipindi hivi. Ikiwa kutakuwa na hatari ya mamlaka kutaifisha simu yako, au kukulazimisha ufungue simu yako na kuonyesha vilivyomo (wakati mtandao umezimwa au vinginevyo), tumia simu nyingine tofauti na ya kwako kuchua taarifa. Hii inaweza kusaidia kupunguza taarifa unazobeba ambazo zinaweza kuathirika

(kwa mfano, namba ulizotunza kwenye simu yako, meseji zako, akaunti zako, n.k). Kama huwezi kutumia kifaa kingine, bado unaweza kufuata muongozo huu ili kupunguza kiasi cha taarifa nyeti na kuimarisha ulinzi kwenye simu yako ya awali.

Ikiwa unataka kubadilisha matumizi ya simu ya zamani, ifute kwanza

Kufuta vilivyomo, futa mpangilio wa simu iliotoka nao kiwandani.

Zingatia: [Tafiti](#) zimeonyesha kuwa kufuta mpangilio simu iliotoka nao kiwandani hakufuti kila kitu. Kwa kweli, njia sahihi ya kufuta kila kitu kwenye simu ni kuiharibu simu husika, lakini njia hii haisaidii kama unataka kuitumia simu tena! Katika [andiko hili](#), injinia wa Adroid alishauri kuhakikisha maudhui ya simu yako yamesimbwa kabla ya kufuta mpangilio ambao simu iliotoka nao kiwandani. Kusimbwa ni huwa ipo moja kwa moja kwenye simu za siku hizi, lakini kama haipo, nenda kwenye mpangilio > Ulinzi > Kusimbwa simu kabla ya kuseti upya. Kwa njia hii, unapofuta kila kitu kwenye simu, funguo za kusimbwa hupotea, na kila data ambayo haijafutika haitaweza kusomwa tena

Fanya mazoezi ya msingi ya ulinzi wa simu

Kuna mazoezi ya ujumla kuhusu ulinzi wa simu ambayo yana husika katika kila hali, iwe unachukua taarifa wakati mtandao umezimwa au la. [Hizi hapa ni baadhi ya mbinu muhimu kutoka](#) kwenye [mashirika mengine](#) Japo hakuna njia ambayo itakuhakikishia usalama kwa 100%, baadhi ya vitu muhimu ni pamoja na:

- Hakikisha umesimba simu yako. Simu mpya zinakuwa zimesimbwa kwa kwa chaguo la msingi tangu awali. Kama huauna uhakuka na ya kwako, angalia mipangilio ya usalama kwenye simu yako.
- Mara kwa mara sasisha mfumo wa uendeshaji (OS), kwa kuwa mara kwa mara hurekebisha hatari za kiusalama.
- Sasisha aplikesheni zako muhimu (kama aplikesheni ya meseji) mara kwa mara.
- Weka neno la siri imara ambalo lina tarakimu 6 na halitegemei alama za vidole/kugusa au kitambulisho wa uso.
- Zima huduma ya kuonyesha eneo ulipo kama huitumii (pamoja na huduma ya dharura ya kuonyesha ulipo, usahihi wa eneo ulilopo, historia ya eneo ulipo, na vipengele vya kusambaziana vya eneo ulilopo, na WiFi na uchaguzi wa skana za Bluetooth). Pia angalia ruhusa ya eneo ulilopo kwenye kila aplikesheni.
- Zima Bluetooth na WiFi wakati huzitumii, ili kukwepa kifaa chako kufuatiliwa.
- Zima simu wakati huitumii.

Sakinisha aplikesheni muhimu za kuweka nyaraka

Kuweka nyaraka za picha au video, unaweza kutumia aplikesheni ya kamera iliyo undiwa kwenye simu yako, au unaweza kutumia aplikesheni maalum kwa ajili ya kuweka nyaraka, kama [ProofMode](#) au zingine, ambazo huruhusu kunasa na kutuma dataelezi nyingi zaidi, pia kutambua na kuthibisha, kusimba, hifadhi salama, au vipengele vingine.

Aplikesheni muhimu kwa ajili ya kuweka nyaraka yenyewe ni [OONI Probe](#), ambayo ni aplikesheni huru kutumiwa na mtu yeyote ambayo hufanya majaribio kutoka kwenye simu yako kupima kama tovuti au majukwaa yanakuwa yamezuiwa. Inaweza kukuonyesha jinsi, wakati, na

ni tovuti gani zimezuiwa. Uwe na uhakika kuelewa [hatari kubwa](#) zilizopo kabla ya kutumia aplikesheni.

Huna uhakika utumie aplikesheni ipi au zipi za kuweka nyaraka? Tunatoa maswali ya kukuongoza katika mafunzo yetu, [Naweza kutumia aplikesheni hii ya kuweka nyaraka?](#)

Sakinisha baadhi ya aplikesheni za kila siku

Kuwa taarifa chache sana na aplikesheni chache maalum kwenye simu yako kunaweza kuamsha wasiwasi. Kufanya simu ione kane kama ni simu ya kila siku, sakinisha aplikesheni za kila siku ambazo ni za kawaida katika eneo unalo chukua nyaraka (lakini ziwe zimepakuliwa kutoka katika vyanzo vya kuaminika), na chukua baadhi ya picha zisizo na makuu au za kawaida kabisa kwa ajili ya hifadhi yako ya picha.

Kwa aplikesheni za mitandao ya kijamii, unaweza kutamani kutengeneza na kufungua akaunti mbadala, ingawaje unatakiwa ukumbuke kuwa akaunti bandia zinakiuka masharti ya huduma katika majukwaa mengi, na tambua mahitaji yanaweza kuthibitika kwa baadhi ya majukwaa yanaweza kufanya ione kane ngumu kutengeneza akaunti bandia. Pia, unaweza kuhitaji kutumia muda mwingi kutengeneza maudhui na kuongeza marafiki, ambapo inaweza kuwa kazi kubwa sana.

Kusasisha aplikesheni wakati hakuna mtandao

Kupakua na kusasisha aplikesheni bila kuwa na mtandao bila shaka ni ngumu. Unahitaji upakue aplikesheni kabla kama unahisi mtandao utazimwa.

Mbinu moja ambayo inaweza kukusaidia pamoja na wengine baadaaye ni kupakua na kuhifadhi kifurushi cha mafaili ya Android (.apk) kwa ajili ya aplikesheni (**zilizo pakuliwa kutoka katika vyanzo vinavyo aminika**, mfano, moja kwa moja kutoka kwa mtengenezaji) katika simu hifadhi ya simu yako au katika flashi. Kuwa na aplikesheni hizi (APKs) nje ya mtandao zitakuruhusu wewe au wengine kusambaziana aplikesheni wakati hakuna mtandao.

Japokuwa hatujapata nafasi ya kujaribu, aplikesheni ya [F-Droid](#) inawezesha kubadilishana Aplikesheni hizi bila kuwa na mtandao. Haya hapa [mafunzo](#) yake.

Tunza taarifa zako binafsi / taarifa nyeti nje ya kifaa chako

Jitahidi kuacha kifaa chako kiwe kwa ajili ya kuchukua nyaraka tu. Usitumie kutuma barua pepe, kupiga simu, au kutuma meseji kwa watu wako binafsi au wanaharakati ambao unaweza kuwaweka kwenye hatari, na usiunganishe vifaa hivi kwenye akaunti zako za msingi na za kweli.

Tumia vipengele vinavyo zuia maudhui

Ikitokea simu yako ikapekuliwa, inaweza kusaidia kupunguza udhahiri wa nia yako, au kufanya kuwa ngumu kutafuta maudhui yako. Ikiwa unahisi mazingira fulani ambayo unahisi simu yako inaweza kupekuliwa kwa haraka, unaweza kutumia mbinu hizi:

- Kubadilisha majina na vifupisho vya ikoni za aplikesheni zako kwa kutumia aplikesheni za kuanzisha (mfani, [Nova Launcher](#), lakini zipo nyingi) kwa hiyo inakuwa vigumu kugundua aplikesheni husika ni ipi.
- Tumia vipengele vya usiri vilivyo undiwa kwenye simu kama [Hali ya Ubinafsi](#) (Samsung) au [Kifungia Maudhui](#) (LG), kama simu yako ina ikubali.
- Kuweka faili lisilo kuwa na kitu ndani linaloitwa “hakunataarifa” ndani ya folda lolote kuzuia taarifa ndani ya folda kutokea kwenye hifadhi ya kwenye simu yako. Kama taarifa bado zitatokea, utapaswa kufuta akiba ya hifadhi ya simu yako. Hii inaweza isifanye kazi mfululizo kwenye simu zote.
- Tengeneza mafolda yaliyo fichwa (mafolda yanoanza “.”) kwa kutumia aplikesheni simamizi. Unaweza pia kuhamisha mafaili kwa kutumia mikono yako kwenda kwenye mafaili yaliyo fichwa au kama unatumia aplikesheni ya kamera kama [kamera ya wazi](#). Unaweza kuamua ni wapi taarifa uliyorekodi itahifadhiwa. Hakikisha unazima chaguo la “onyesha mafaili yaliyofichwa” katika mpangilio wa simu yako ili mafaili yaliyo fichwa yasionekane.
- Baadhi ya aplikesheni maalumu kwa ajili ya kuchukua nyaraka, kama [Tella](#) au [Eyewitness to Atrocities](#), hutunza nyaraka katika hifadhi tofauti ziliyo simbwa ambazo taarifa zake hufikika ndani ya aplikesheni tu, ambayo hufanya iwe vigumu kwa mtu anayepekua taarifa zako. Kuweka nyaraka katika hifadhi hizi salama huhitaji neno la siri lingine kwenye aplikesheni, ili ibaki imesimbwa na hata kama simu yako itafunguliwa.

Vitu muhimu kuhusu kuzuia maudhui yako

Ni muhimu kuzingatia kuwa njia hizo hapo juu zinaweza kutosha kumzuia mtu anaye pekua simu yako kwa haraka, lakini **hazisaidii kama mtu ameamua kukagua simu yako kwa umakini kabisa.**

Pia kumbuka kuwa baadhi ya nchi zina sheria zinazozuia au kufanya kuwa kosa la jinai matumizi ya aplikesheni za usalama zilizo simbwa au kufuta data. Kuzitumia kuzuia mamlaka kupekuwa taarifa zako kunaweza kuonekana kama kuharibu ushaidi au kuingilia uchunguzi, na labda huenda ukaadhibiwa kama mhalifu. [Ramani](#) hii (pana, lakini ni ya 2017) inatoa sehemu nzuri ya kuanzia kama una maswali kuhusu sheria za nchini kwako.

Kuseti kwa ajili ya kusambaziana wakati hakuna mtandao

Katika mazingira ambayo hauna mtandao baada ya kuchukua maudui yako, unaweza bado kuhitaji kuyatoa kwenye simu yako kwa ajili ya sababu za kiusalama, kupunguza nafasi kwenye simu yako, au kusambaziana na wengine. Mara nyingi kutoa nyaraka kwenye simu yako pia husaidia kupunguza taarifa zinazoweza kuharibiwa kwenye simu yako ikiwa itataifishwa au kufunguliwa.

Hata kama huwezi kuunganisha na matandao, bado unaweza kuunganisha na WiFi au Bluetooth za vifaa vingine kienyeji, kama vile simu nyingine au flashi ya WiFi USB. Simu yako inapaswa kuja na aplikesheni au mpangilio unao kuwezesha kuunga na kuhamisha. Kama simu yako inakubali, unaweza kuchomeka flashi ya USB ya OTG au kiungo ili kuhamisha nyaraka kwenda kwenye flashi nyingine ya OTG au kifaa kingine.

Njia hizi zimeelezewa zaidi katika mafunzo yetu ya [Kusambaziana faili na kuwasiliana wakati mtandao umezimwa](#) na karatasi yetu ya [vidokezo ya Video Kama Ushahidi:Vifaa vya Kiteknolojia – Kuhamisha Mafaili](#).

Fanya mazoezi kabla hujaingia katika hali ya mgogoro

Seti simu yako sasa kama una mtandao au wakati utakapo kuwa na mtandao. Anza kufanya mazoezi ya kutumia hizi aplikesheni katika hali ya kila siku (wakati hakuna hali yoyote inayo hatarisha usalama) ili kwamba uwe umezizoea na kujisikia vizuri kuzitumia. Fanya ulinzi mzuri wa msingi mzuri wa simu yako uwe ni chaguo la mazoezi yako ya msingi. Kwa njia hii kanuni Mbinu hizi zitakuwa na kawaida kwako wakati utakapo kuwa kwenye hali ya mgogoro huku ukiwa na mambo mengine ya kuhofia.

Naweza Kutumia Aplikesheni hii ya Kuweka Nyaraka?

Imehakikiwa mwisho: 31 January 2020

Kuna aplikesheni nyingi ambazo wachukua nyaraka wanaweza kutumia kwa kunasa video, ambapo inaweza kuwa ni [aplikesheni ya kamera ya simu](#) yako, aplikesheni maalum kwa ajili ya kuchua nyaraka kama vile [ProofMode](#), [Tella](#), au [Eyewitness to Atrocities](#). Baadhi ya aplikesheni zina vipengele vinavyo tegemea mtandao, hivyo ni vema ukakumbuka kuwa vipengele hivyo havitakuwepo ikwa mtandao utazimwa.

Hatuwezi kukuambia ni aplikesheni ipi itakufaa wewe, kwa kuwa hilo lina tegemeana na hali yako, mahitaji yako, na hatari zilizopo (angalia makala hii kwa maelezo zaidi kuhusu [jinsi ya kupima migogoro na hatari](#)). Ukiwa na tathmini ya hatari zilizopo mkononi, haya maswali ya mwongozo hapa chini yanaweza kukusaidia kutathmini ni aplikesheni ipi ya video inayoweza kuwa nzuri zaidi kwako.

Ni nani aliye tengeneza aplikesheni na nitawaamini je?

Mara zote zingatia kujua watengenezaji wa aplikesheni yoyote ile unayotaka kupakua na kusakinisha kwenye kifaa chako, na kama unaweza kuwaamini kuwa hawakuweki hatarini, kwa makusudi au bila kukusudia.

Baadhi ya vitu vya kuzingatia ni:

- Mtengenezaji wa aplikesheni ana sifa nzuri? Watu wa jamii yako na walio katika mitandao mikubwa wanasema nini kuhusu wao na vifaa vyao?

- Je, mtengenezaji wa aplikesheni yuko hatarini kushambuliwa? Zingatia sifa zao na uwezekano wa kulazimishwa kutoa data zako au kuweka mwanya wa mamlaka (au kama walisha wahi kufanya hivyo awali). Ni nchi gani data zako zimehifadhiwa na ni sheria zipi zinazo husiana na amri za mahakama nchini humo?
- Je, mtengenezaji wa aplikesheni ana iboresha? Vifaa visivyo boreshwa viko hatarini kuvamiwa na wadukuzi wa mitandaoni kama wakigundua mwanya uliopo. Angalia tovuti ya mtengenezaji au kurasa zake za aplikesheni kutoka hifadhi ya Google Play uone tarehe ya “mwisho ilipo sasishwa.”
- Mtengenezaji wa aplikesheni amejiimarisha kwa kiasi gani, na je wanaonekana wataiendeleza aplikesheni yao kwa muda mrefu?
- Je, aplikesheni hiyo ni huru wa kila mtu kutumia? Aplikesheni ambazo ni huru kudadisiwa zinauwezekano mkubwa wa masuala yao ya kiusalama kujadiliwa au angalau kutambuliwa. Je mtengenezaji ameweka wazi ubora na usalama wa aplikesheni?
- Ni motisha gani au vivutio vipi vilivyo mvutia mtengenezaji wa aplikesheni, na ni kwa jinsi gani vinaweza kupelekea uaminifu wake? Kwa mfano, je wana malengo? Wana lenga faida? Wanafadhiliwa na mhisani fulani?
- Japokuwa sio kipimo cha moja kwa moja cha uaminifu wao au la, gharama ya aplikesheni zinaweza kuwa ni jambo la kuzingatia. Aplikesheni zingine zina malipo ya juu ya kila mwezi au malipo ya video moja moja.

Kwa habari zaidi angalia [EFF](#) ambapo ni mwongozo wa uangalizi wa ulinzi binafsi katika [kuchagua aplikesheni](#).

Aplikesheni zinapakuliwa kutoka wapi?

Mara zote unapaswa kupakua na kusakinisha aplikesheni kutoka katika hifadhi za aplikesheni au tovuti zinazo aminika. Hata kama umefanya utafiti wa kina kuhusiana na kuaminika kwa aplikesheni, hifadhi za aplikesheni zisizo kamili zinaweza kukupotosha na kujikuta umepakua aplikesheni haramu ambayo imetengenezwa kwa nia mbaya. Kwa mfano mwaka jana shirika la kupigania haki za mitandaoni [SMEX](#) ilitoa [onyo](#) kuhusu tovuti mbalimbali zilizokuwa zina tangaza aplikesheni inayoitwa “WhatsApp Plus” (kuweka mambo wazi, hii si bidhaa ya WhatsApp!), ambayo inaweza kuhifadhi na kuuza data za watumiaji, au kusababisha simu zilizo sakinisha kutapeliwa mtandaoni.

Baadhi ya watengenezaji walio makini na usalama hutoa funguo za kriptografia ambazo hukuwezesha kuthibitisha uhalali wake. Mara zote hutoa maelezo ya jinsi ya kuthibitisha saina hizo.

Data zitakuwa zimehifadhiwa wapi?

Baadhi ya aplikesheni za kuweka nyaraka huhifadhi data na nyaraka kwenye kifaa chako kienyeji, huku baadhi tu ndio hutuma na kuhifadhi data kwingineko. Mara nyingi hii inatokana na na muundo na nia ya aplikesheni husika, kama vile aplikesheni ya Eyewitness to Atrocities,

ambayo hutuma nakala halisi ya nyaraka yako kwenda kwenye hifadhi ya Lexis Nexis ili Eyewitness iweze kuhakiki mnyororo wa ulinzi na uhalisia wa taarifa husika. Unaweza kuhamisha taarifa yako kutoka hifadhi iliyosimbwa kwenye simu yako ndani ya aplikesheni ya Eyewitness tu *baada* ya kutumwa kwa ajili ya ulinzi.

Chaguo ni lako kuamua kama unataka kuacha nyaraka zibaki kwenye simu yako pekee, au kama unataka kutuma na kuhifadhi sehemu ya mbali ambayo utaweza kuidhibiti (kama ilivyo ni chaguo katika [Tella](#)), au kama utahitaji kutuma kwenye mashirika ya nje / majukwaa ambayo umeyaruhusu kufikia na kutumia nyaraka zako. Kumbuka kuwa wakati wa kuzimwa mtandao, hutaweza kutuma nyaraka zako mtandaoni wakati huo huo, hivyo utahitaji aplikesheni ambayo itakusaidia angalau kuhifadhi nyaraka zako kienyeji kwa muda (na kuziweka chelezo vizuri) (Angalia [Kuweka chelezo data za simu bila kuwa na mtandao au kompyuta](#)).

Iwapo data zako zitatumwa eneo la mbali, fahamu ni nchi gani ambayo data zako zitakuwa. Kuna hatari gani ya data kufichuliwa katika nchi hizo, iwe ni kwa amri ya mahakama au namna nyingine? Ni hatari gani utapata kama data zako zikifichuliwa huko?

Je aplikesheni husimba taarifa zangu?

Baadhi ya aplikesheni, kama Tella na Eyewitness to Atrocities, huwa na uwezo wa kusimba mafaili au/na hifadhi iliyosimbwa kwa ajili kuweka nyaraka zako, ambayo ni tofauti na hifadhi ya simu yako na kusimbwa kwa simu yako, ili kwamba taarifa zako na dataelezi za simu yako kamwe zisitoke katika hali ya kusimbwa hadi pale zitakapo fikiwa kwa kutumia aplikesheni yenye neno la siri. Hii inamaanisha kuwa hata kama simu yako imetolewa neno la siri, nyaraka zako zina endelea kuwa zimesimbwa. Hii inatoa viwango vingine vya ziada vya usalama kwa nyaraka zako.

Kama aplikesheni itatuma na kuhifadhi taarifa zako eneo la mbali baada ya mtandao wako kurudishwa, pia fikiria iwapo unahitaji taarifa zako zisimbwe zikiwa njiani na zikiwa eneo la mbali, kwa mfano kama vile aplikesheni ya EyeWitness inavyofanya..

Kumbuka kuwa japokuwa usimbaji ni halali katika maeneo mengi, baadhi ya nchi zinaweza kuwa na sheria ambazo huzuia au kufanya kuwa ni kosa la jinai matumizi ya usimbwaji. [Ramani](#) hii (ya jumla, lakini ya kutoka mwaka 2017) inatoa sehemu nzuri ya kuanzia kama una maswali kuhusiana na sheria za nchini kwako.

Je aplikesheni inanasa dataelezi (bila mtandao)?

[Dataelezi](#) ni data ambazo huelezea video au picha yako, kama vile muda na tarehe au eneo. Taarifa hii ni muhimu kwa kutambua, kuelewa, kuhakiki, na kuthibitisha video au picha kama nyaraka ya tukio fulani. Katika mazingira ya mtandao kuzimwa, uwezo wa aplikesheni kukusanya dataelezi fulani moja kwa moja na/au kukuruhusu kuweka maelezo ya taarifa kiurahisi papo hapo ni muhimu sana, kwa kuwa inaweza kuchukua muda mrefu kabla ya kusambaziana nyaraka na yeyote yule (wakati ambapo taarifa zinaweza kusahauhulika, hali kubadilika, n.k, n.k).

Aplikesheni nyingi za kuchukua nyaraka kama vile ProofMode zina vipengele bora vya dataelezi, na hucusanya dataelezi nyingi kuliko aplikesheni za kamera zilizo undiwa kwenye simu. Dataelezi iliyo boreshwa inaweza kujumuisha taarifa mbalimbali zilizo kusanywa kwenye mawimbi ya wifi au bluetooth, data za simu, heshi ya kripografia, na taarifa iliyo sambazwa na mtumiaji, ambapo zote zinawezesha uhakiki na uthibitisho wa taarifa baadaye.

Kumbuka kuwa wakati mtandao umezimwa, utahitaji aplikesheni ambayo haihitaji data ili kutoa au kurekodi dataelezi. Baadhi ya aplikesheni zina tegemea mtandao, badala ya vifaa vya sensor, ili kukusanya dataelezi fulani. Mfano, iwapo data za eneo zimenaswa kupitia mpangilio wa simu, dataelezi huenda zikaangazia eneo la mwisho ambalo simu ilikuwa na mtandao, badala ya mahali halisi kilipo kifaa. Aplikesheni hii pia inatakiwa ikuruhusu kuhifadhi dataelezi zako kienyeji bila kuwa na mtandao, pamoja na kuhifadhi fomu yoyote ambayo unajaza (mfano, “Hali ya bila mtandao” ya Tella).

Naweza hamisha data kutoka kwenye aplikesheni?

Kutegemeana na nia yako ya kuweka nyaraka, itakuwa inafaa kuweza kuhamisha nyaraka za video na dataelezi kutoka kwenye aplikesheni, kwa mfumo ambao si wa umiliki wa aplikesheni; yaani, kuweza kufungua, kuangalia, na kutumia taarifa na dataelezi nje ya aplikesheni. Uwezo wa kuweza kuhamisha ina maanisha kuwa wewe na wengine hamtegemei aplikesheni moja au mtoa huduma mmoja ili kuzipata nyaraka zako, na inakupa uhuru mkubwa kufanya kazi zako kusonga mbele. Kumbuka kuwa baadhi ya dataelezi haziwezi kueleweka kama hauna uwezo wa kufikia datamsingi au chati fulani kufafanua namba (kwa mfano, kama utambulisho wa minara ya simu au mitandao ya Wi-Fi).

Kumbuka baadhi ya aplikesheni zinaweza kuwa na minyororo ya uangalizi iliyo fungwa makusudi na hairuhusu watumiaji kuhamisha, huku baadhi ya aplikesheni zikiwa hazikuundwa kwa kusudi la kuhamisha. Pia kumbuka kuwa baadhi ya aplikesheni kama Eyewitness to Atrocities, haita kuruhusu uhamishe hadi uwe umepakia taarifa zako kwenye seva ya mbali (ambapo unahitaji mtandao ili kufanya hivyo), na baadhi ya aplikesheni zinaweza kukuruhusu kuhamisha taarifa, lakini si dataelezi (mbali na dataelezi zilizo kwenye faili husika).

Iwapo unataka kuhamisha, kimsingi aplikesheni yako sharti ikuruhusu kuhamisha nakala ya taarifa bila mabadiliko yoyote na nakala ya dataelezi ikiwa katika kiwango cha maandishi ya meseji yanayo someka. Kwa mfano dataelezi ya Tella, ina hifadhiwa ikiwa imesimbwa katika hifadhi ya Tella, lakini inaweza kuhamishwa kama CSV. Pia, wakati mtandao umezimwa, ni muhimu kuwa na njia mbadala ya kuhamisha kwenye aplikesheni zisizo hitaji mtandao au huduma zisizo tegemea mtandao. Idadi kubwa ya aplikesheni zinazo kuruhusu kuhamisha zina kitufe cha “Sambaza” ambacho kinachochea menu ya usambazaji, ambayo Android imejaza na orodha ya aplikesheni katika simu yako ambazo zina uwezo wa kushughulikia aina hiyo ya maudhui. Bahati mbaya watengenezaji wa aplikesheni wanaweza kubadilisha menu za kusambaza na hakuna mfululizo katika aplikesheni tofauti tofauti.

Kwa idadi kubwa ya mafaili, itakuwa vizuri zaidi kufikia mafaili yaliyo hifadhiwa kupitia aplikesheni simamizi za mafaili na kunakili faili kutoka hapo, japokuwa hauta weza kufikia dataelezi zilizo hifadhiwa katika datamsingi za aplikesheni kwa njia hii. Chaguo hili pia halipo kwenye aplikesheni ambazo hujisimamia usalama wa hifadhi zao, kwa vile mafaili yanakuwa yamesimbwa katika kutunza. Kwa aplikesheni hizi, ni muhimu kuwa na uwezo wa kusambaziana ndani ya aplikesheni.

Kudumisha Taarifa Zinazo weza Kuthibitika Wakati Mtandao Umezimwa

Makala hii ni sehemu ya mfululizo kwenye [Kuchukua Nyaraka Wakati Mtandao Umezimwa](#).

Ili hakikiwa mwisho: 31 Januari 2020

[Watetezi wa haki za binadamu](#), [wapelelezi](#), [watafiti](#), na [wanahabari](#) mara nyingi hutegemea nyaraka za mwanzo ambazo zilinaswa na mashahidi kufuatilia, kuripoti, na kuongolelea ukiukwaji wa haki za binadamu. Ili kuhakikisha kwamba wanafanyia kazi taarifa sahihi, watumiaji huchukua hatua ya kutafuta uhalali na kuthibitisha nyaraka wanazo pokea, mchakato ambao unaweza kuwa na machungu na hutumia muda mwingi.

Kama mchukua nyaraka, kuna vitu virahisi unaweza kufanya ili kurahisishia wengine kazi ya kuthibitisha na kuhakiki nyaraka, ili iweze kutumika kwa wakati na kwa ufanisi. Njia hizi chache za ziada ni muhimu zaidi wakati mtandao umezimwa, ukizingatia kuwa:

- Kama hautaweza kupakia muda huo huo, tarehe ya uchapishaji na taarifa ya eneo inayo tolewa katika mitandao ya kijamii haisaidii kwa kuonyesha kuwa video yako ilinaswa tarehe husika au kabla ya tarehe fulani au katika eneo fulani.
- Iwapo wengine pia hawawezi kupakia, huenda kukawa na uwekaji nyaraka mdogo kwa ujumla ambao utaweza kutumiwa kuthibitisha video yako.
- Kama utahitaji kupitisha video yako kwenye mikono mingi bila kuwa na mtandao ili kufika sehemu iliyo kusudiwa, inaweza kuwa ngumu kwa wengine kufuatilia chanzo cha video hiyo.
- Iwapo unataka kufuta video asilia kutoka kwenye simu yako kwa sababu za kiusalama au nafasi kidogo ya kuhifadhi bila kuwa na chelezo mawinguni, au iwapo unataka kuacha kuitumia simu yako, huenda ikawa vigumu kuthibitisha uhalali wa video.
- Iwapo umesahau maelezo kuhusu video fulani na aplikesheni unayo tumia hainasi / kurekodi dataelezi bila kuwa na mtandao, wengine hawataweza kuitambua baadaye.

Vidokezo vifuatavyo vinaweza kukusaidia kudumisha video yako wakati mtandao umezimwa ili kuongeza uwezekano wa kuthibitika na kutumika kama nyaraka baadaye.

Nasa au toa maelezo ya kutambulisha kwenye video

Jitahidi katika video zako uweke maelezo ambayo yatamrahisishia mpelelezi au mwanahabari baadaye kutambua wakati na eneo, kama vile upekee wa maeneo, anga, alama za mitaani,

mbele ya maduka, mabanda ya leseni, bendera, saa, kurasa za mbele za magazeti, n.k. Unaweza pia ukasimulia taarifa muhimu kama vile jina lako, na taarifa zako za mawasiliano (iwapo ni salama kufanya hivyo), muda, tarehe na eneo/alama za GPS (au kuandika kwenye karatasi na nasa hiyo karatasi). Unapotoa maelezo mengi, ndivyo itakavyo kuwa rahisi kwa mtu mwengine kutafiti na kuthibitisha hiyo video baadaye, hata kama hawakujui au hawajui ni wapi hiyo video ilitoka. Angalia vidokezo vyetu kwenye [Mafunzo ya Msingi ya Kunasa, Kuhifadhi na Kusambaza](#) kwa mengi zaidi.

Ongeza maelezo / dataelezi

Tumia fursa ya moja ya aplikesheni nyingi zilizo jikita katika kuweka nyaraka ambazo huvuta dataelezi au taarifa za kiufundi kutoka katika simu yako, na huruhusu kuweka taarifa za maelezo ya ziada kwa njia ya kawaida. Kumbuka kwamba, wakati wa kuzimwa, unahitaji aplikesheni ambayo hakitegemei mtandao ili kurekodi au kuhifadhi dataelezi. Angalia [“Naweza Kutumia Aplikesheni Hii kuchukua Nyaraka?”](#) kwa habari zaidi jinsi ya kuchagua aplikesheni inayofaa.

Hata kama hutumii aplikesheni iliyo jikita katika kuchukua nyaraka, bado unaweza kutengeneza taarifa za ziada kwa njia ya muhtasari, ramani, au picha katika simu yako. Unaweza panga video zako kwa kutumia maelezo haya ya ziada huku ukitumia aplikesheni ya kusimamia mafaili unayo ipendelea. Maelezo muhimu ya ziada ya kuweka ni pamoja na , muda, tarehe, eneo kuliko rekodiwa kisa husika, pia chanzo cha rekodi hiyo. (yaani, jina lako na mawasiliano yako) iwapo ni salama kujumuishwa. Hamisha dataelezi na jumuisha na video (unaweza kuziweka zote kwenye folda na ufunge) wakati unapo sambaza.

Weka Chelezo

Weka chelezo ya taarifa zako kutoka katika simu yako kila mara, hasa kwenye hifadhi 2 na iwe kwenye vifaa tofauti. Unaweza, kwa mfano, kuunganisha kwenye On-the-Go (OTG) au flashi isiyochoekwa kwenye simu yako, hata bila kompyuta. Angalia vidokezo vyetu kwenye [Kuweka chelezo taarifa za simu bila kuwa na mtandao au kompyuta](#)” kwa maelezo zaidi. Kuweka chelezo itahakikisha kwamba unabaki na nakala ya video yako iwapo utapoteza au simu yako kuvunjika, au unataka kufuta video kutoka kwenye simu yako. Kuwa na nakala asili ya video iliyo salama pia ina muwezesha mpelelezi au mwanahabari ambaye atakuwa ameona video yako kupitia njia nyingine kupata video hiyo moja kwa moja kutoka kwako baadaye (ili mradi wawe wanaweza kuifuatilia hadi kwako), kuandaa mnyororo wa usimamizi ulio mfupi na ulio kamili.

Kuweka Chelezo Taarifa Zilizo Kwenye Simu Bila Kuwa na Mtandao au Kompyuta.

Makala hii ni sehemu ya mfululizo wa [Kuweka Nyaraka Wakati Mtandao Umezimwa](#).

Imehakikiwa mwisho: 31 Januari 2020

[Kuweka chelezo](#) ni muhimu kwa kuhakikisha kuwa data na nyaraka hazifutwi kwa bahati mbaya, kuharibika, au kupotea iwapo simu yako imetaifishwa. Wakati mtandao umezimwa au umezuiliwa kwa kiasi, huenda usiweze kuendelea kuweka chelezo mawinguni au kutuma nyaraka zako katika eneo la mbali na ulipo. Kuweka katika kompyuta ya mezani au kompyuta mpakato ni njia mojawapo ya kuweka chelezo, lakini kwa vile watu mara nyingi hawana njia ya kupata kompyuta, hapa kuna baadhi ya njia na vidokezo vya kuweka chelezo ya taarifa kutoka kwenye simu yako wakati wa mtandao umezimwa na hauna kompyuta.

Tumia OTG au flashi

OTG, au on-the-go, flashi ni aina ya USB ambazo zinawiana na Androids nyingi (lakini si zote). Unaweza kuunganisha flashi ya OTG moja kwa moja kwenda kwenye simu yako, au utumie adapta ya OTG kwenda USB ili kuunganisha simu yako kwa USB ya kawaida. Ukiwa na OTG, simu yako inapeleka umeme kwenye flashi.

Makampuni maarufu ya flashi za OTG ni pamoja na SanDisk, Kingston, na Samsung, japokuwa kuna nyinginezo. Kawaida zina gharimu US\$8-\$25 kutegemea na uwezo wake wa kutunza data. Flashi zisizo chomekwa / flashi ngumu ni sawa na flashi za kawaida ila hazihitaji waya. Hii itakuruhusu kuunganisha kwenye simu ambazo kwa kawaida haziunganishi kwenye flashi, kama vile simu yako. Faida ya flashi isiyo chomekwa dhidi ya flashi ya OTG ni kwamba unaweza kuunganisha vifaa vingi kwenye flashi hiyo kwa wakati mmoja. Hii itakuwa ya msaada, kwa mfano, katika maandamano ambapo mnachukua matukio kwa video kama kikundi, na taarifa ya kila mmoja itawekwa chelezo kwenye flashi aliyo nayo mwenzako. Kumbuka kuwa kwa sababu hazitumii umeme kutoka kwenye kifaa, flashi zisizo chomekwa zinategemea umeme ya betri na zinatakiwa kuchajiwa.

SanDisk ina wezekana ndio kampuni maarufu ya flashi zisizo chomekwa, japokuwa kuna makampuni mengine. Flashi zisizo chomekwa ni ghali zaidi kuliko flashi za OTG, na zina anzia US \$25-\$100 kutegemea na uwezo wa viwango vya kuhifadhi. Flashi ngumu za nje zisizo chomekwa zina anzia US\$150 kulingana na uwezo wa viwango vya kuhifadhi.

Njia mbadala: Tumia simu ya zamani ambayo haijawahi kutumika

Iwapo hauna OTG au or flashi isiyo chomekwa, lakini una simu ya zamani ambayo bado inafanya kazi na huitumii, unaweza pia kuitumia kuweka chelezo. Ikiwa simu zote ziko katika umbali wa kukaribiana, unaweza kuunganisha na kunakili taarifa kutoka moja kwenda nyingine kwa kutumia Bluetooth, WiFi ya moja kwa moja, au Mawasiliano ya karibu (NFC) / Android Beam. Bluetooth na Wifi ya moja kwa moja zote ni teknolojia zisizo chomekwa ambazo zinaweza kuunganisha vifaa viwili bila kiunganishi cha mtandao (router) au kitovu cha kuunganisha mtandao kati ya zenyewe. WiFi moja kwa moja hutoa nafasi pana na uhamishaji

wa data wa kasi ya juu kuliko Bluetooth, lakini hutumia umeme mwingi. Vilevile, NFC ina nafasi ndogo (~sm4) na kasi ya chini ya kuhamisha kuliko Bluetooth au WiFi ya moja kwa moja, lakini hujiunganisha haraka na hutumia umeme kidogo, hivyo inaweza kuwa ya manufaa kwa uhamishaji mdogo mdogo wa haraka wakati una vifaa vyote mkononi.

Simu yako bila shaka ina Bluetooth, WiFi moja kwa moja, au vipengele vya NFC kwenye aplikesheni ambavyo vina kuruhusu kuchagua kifaa kilicho karibu ili uweze kukisambazia taarifa. Iwapo simu zote zina Files By Google ambazo zimesakinishwa, unaweza pia kusambaziana mafaili bila mtandao kwa kutumia teknolojia iliyopo kwenye aplikesheni.

Muhimu: ubaya wa uunganishaji huu wa rahisi ambao unatolewa na huduma hizi haupo salama. Bluetooth na skana za wifi zinaweza kutumika kufuatilia eneo ulipo au kuchunguza taarifa katika kifaa chako. Matapeli wanaweza kujaribu kujiunganisha na kifaa chako, kukutumia mafaili usiyo hitaji, au kupata nafasi ya kudhibiti kifaa chako kama kipo hatarini. **Ili kuwa salama, funga huduma hizi wakati hauzitumii na uwashe tu wakati uko katika maeneo salama, zuia ruhusa kwenye aplikesheni zako na ukubali tu kwenye zile una hitaji/Yule unamhitaji, na tekeleza usalama wa simu ulio bora kama vile kusasisha na kuwa na neno la siri imara.**

Jumuisha maelezo yoyote ya pembeni/dataelezi

Wakati una nakili taarifa kwenda katika flashi ya OTG, flashi isiyo chomekwa, au simu ya zamani, ni vizuri kujumuisha taarifa za kuelezea au dataelezi ambazo zitakuwa tofauti na taarifa. [Aplikesheni za nyaraka](#), zilizo nyingi kwa mfano, hutoa nyaraka za maandishi za CSV au JSON ambazo hujumuisha dataelezi zilizo tolewa kwenye simu (mfano, .jiografia ya eneo, muda, tarehe) na maelezo yoyote yaliyowekwa na mtumiaji kwa mikono na mtumiaji. Hakikisha kwamba unahamisha na kujumuisha hizi nyaraka za dataelezi kwenye chelezo yako pia.

Neno la siri hulinda flashi

Flashi nyingi zisizo chomekwa zinaweza kulindwa kwa neno la siri kwa kutumia aplikesheni za simu ambazo zinakuja na flashi. Kumbuka kuwa ulinzi wa neno la siri si sawa na usimbwaji (angalia hapo chini). Flashi nyingi zisizo chomekwa au za OTG haziwezi kuruhusu usimbwaji kamili wa diski kwa kutumia simu ya mkononi tu, japokuwa zinaweza ruhusu usimbaji kamilifu wa diski kwa kutumia kompyuta.

Zingatia kusimba mafaili

Iwapo unataka kuhifadhi mafaili yako kwa usalama zaidi, unaweza kuzingatia kusimba chelezo zako. Huku ukiwa hauwezi kusimba flashi nyingi zisizo chomekwa au za OTG kwa kumia simu ya mkononi, unaweza kusimba mafaili kabla hauja zihamishia kwenye flashi. Baadhi ya aplikesheni zinazo weza kusimba mafaili katika Android ni [ZArchiver](#), na [RAR](#). Kumbuka kuwa

sharti ukumbuke neno lako la siri la usimbaji. Hakuna njia ya kupata mafaili yaliyo simbwa iwapo utasahau au kupoteza neno lako la siri.

Kumbuka kuwa baadhi ya nchi huenda zinaweza kuwa na sheria ambazo zinazuia au kufanya kuwa kosa la jinai matumizi ya kusimba. Kutumia kuzuia mamlaka kuingilia taarifa zako kunaweza kuchukuliwa kama kuharibu ushahidi au kutatiza uchunguzi, na inaweza kuadhibiwa kama kosa la jinai. Hii [ramani ya 2017](#) inaweza kuwa imepitwa na wakati lakini inatoa sehemu nzuri ya kuanzia kama una maswali kuhusu sheria za nchini kwako.

Weka chelezo kwenye sehemu 2 tofauti

Kuweka chelezo katika sehemu moja haitoshi kamwe. Kwa mfano, unaweza kupoteza kifaa chako ulichotunzia chelezo, kuharibika, au kinaweza kushindwa kufanya kazi ghafla. Wataalamu wa tehamu wana shauri watu kuwa na chelezo 2 (yaani nakala 3 kwa jumla), kwenye vifaa tofauti vilivyo katika maeneo tofauti. Hii inasaidia kupunguza hatari tofauti tofauti kwenye nakala yoyote ile.

Kusambaziana Faili na Kuwasiliana Wakati Mtandao Umezimwa

Makala hili ni sehemu ya mfululizo kwenye [Kuweka Nyaraka Wakati Mtandao Umezimwa](#).

Mwisho ilihakikiwa: 31 Januari 2020

Uzimaji na ukataji wa mtandao unaoendelea Kashmir, ni uzimaji wa mtandao ulioendelea kwa muda mrefu zaidi katika demokrasia, na umekuwa na [athari mbaya sana](#) kwa maisha ya watu katika ukanda huo. Kuongeza machungu kwenye kidonda, Disemba 2019, [akaunti za WhatsApp za raia wa Kashmiri zilianza kubatilishwa](#) kutokana na watumiaji kushindwa kutumia akaunti zao kwa siku 120 kulingana na sera za WhatsApp.

Wakati wa kuandika makala hii mwezi Januari 2020, Mahakama ya Juu ya India iliamua kuwa uzimaji mtandao huko Kashmir ni [kinyume cha sheria na matumizi mabaya ya mamlaka](#). Mtandao wa kasi na ule wa simu ulirudishwa kwa baadhi ya maeneo, lakini pia ulikuwa una chagua tovuti “zilizo kubaliwa” tu.

Uzimaji mtandao unalenga kuwazuia watu kusambaziana taarifa na kuwasiliana (na pia kulazimisha watu kuwa katika hali ya mawasiliano yasiyo salama sana kama vile simu za mkononi na meseji, ambavyo ni rahisi kwa mamlaka kuingilia na kufuatilia). Kamwe hakuna mbinu nzuri za kutafuta suluhu wakati mtandao umezimwa kabisa. Wakati wa masharti magumu zaidi wa kuzimwa mtandao huko Kashmir, kwa mfano, watu waliamua [kutumia maandishi ya kuandika kwa mkono na huduma za usafirishaji](#) ili kufikisha ujumbe kwa wapendwa wao.

Hatuna njia ya uhakika kabisa ya kuweza kukwepa vizuizi vyote, lakini kupitia mazungumzo na wanaharakati na wenzetu, tumejifunza baadhi ya mbinu na njia za kutumia kwa ajili ya kusambaziana na kuwasiliana zinazoweza kukusaidia wewe, kulingana na hali na mazingira. Kumbuka kuwa baadhi ya njia hizi huhitaji mtandao awali ili kuweza kuseti (mfano, kupakua aplikesheni).

Sambaza mafaili moja kwa moja kwa kutumia Bluetooth, Wifi ya moja kwa moja, au NFC

Hauhitaji mtandao ili uweze kuunganisha simu yako na kifaa kingine cha karibu kwa kutumia Bluetooth, Wifi ya moja kwa moja, au Mawasiliano ya karibu (NFC) (mara nyingine huitwa Android Beam kwenye simu za zamani). Bluetooth na Wifi ya moja kwa moja zote ni njia za teknolojia ambazo hazi hitaji waya na zina uwezo wa “kuunganisha” simu mbili bila ruta au kiunganishi katikati yake. WiFi ya moja kwa moja inatoa nafasi pana na kasi ya juu ya uhamishaji data kuliko Bluetooth, lakini inatumia umeme mwingi. NFC ina nafasi fupi (~sm 4) na kasi ya chini ya kuhamisha kuliko Bluetooth au WiFi ya moja kwa moja, lakini inaunganishika haraka na hutumia umeme kidogo, hivyo basi inaweza kuwa ya manufaa katika uhamishaji mdogo mdogo wakati una vifaa vyote mkononi mwako.

Bila shaka una vipengele vya Bluetooth, WiFi ya moja kwa moja, na NFC ambavyo vimeundiwa kwenye simu yako ambavyo vinajitokeza unapo chagua kusambaza. Na zaidi, aplikesheni zenye vipengele vya kusambaziana mafaili, kama [Files By Google](#), pia huunganisha teknolojia hizi.

Muhimu: ubaya wa uunganishaji huu wa rahisi ambao unatolewa na huduma hizi ni kwamba haupo salama. Bluetooth na skana za wifi zinaweza kutumika kufuatilia eneo ulipo au kuchunguza taarifa katika kifaa chako. Matapeli wanaweza kujaribu kujiungamanisha na kifaa chako, kukutumia mafaili usiyo yahitaji, au kupata nafasi ya kudhibiti kifaa chako kama kipo kwenye hatari. **Ili kuwa salama, funga huduma hizi wakati hauzitumii na iwashe tu wakati uko katika maeneo salama, zuia ruhusa kwenye aplikesheni zako na uruhusu tu kwenye unazo zihitaji na unapo zihitaji tu, na ufanye mazoezi ya kuhakikisha usalama bora wa simu kama vile kusakinisha na kuwa na neno la siri ambalo ni imara.**

Kusambaziana mafaili kwa flashi isiyo chomekwa au kupitia Mtandao wa Eneo Lako (WLAN)

Flashi isiyo chomekwa au flashi ya kuchomekwa inaweza kutumika kusambaziana mafaili miongoni mwa kundi, au watu wengi kwa wakati mmoja. Flashi ya wifi inakuja na maagizo na/au aplikesheni ya kuunganisha simu yako kwenye flashi hiyo, na ni rahisi kutumia. Kumbuka kuweka neno la siri kwenye flashi kwa ajili ya usalama.

Kama hauna flashi isiyo chomekwa, unaweza pia kusambaza mafaili kwa kutumia flashi ya kawaida ya USB kwa kuweka kwenye ruta isiyo chomekwa. Ruta ya kubebea yenye mlango wa USB, kwa mfano, si ghali na inabebeka kiurahisi. Watumiaji wanaweza kujiunganisha kwa kutumia flashi za USB kupitia mtandao wa eneo lao (mtandao hauhitajiki). Ili kuweza kuyafikia mafaili katika flashi ya USB ambayo imeunganishwa kwenye simu yako, utahitaji kutumia aplikesheni ya kusimamia ambayo itakuunganisha kwenye hifadhi ilio unganishwa, kama vile [Solid Explorer](#). Anwani ya IP ya ruta yako itaweza kupatikana kama kawaida katika mpangilio wa WiFi wa simu yako.

Pia, chaguo jingine ni [PirateBox](#), ambayo ni mradi wa jifanyie wewe mwenyewe ambao unatoa mifumo ya programu za leseni bure. Watumiaji wanaweza kusambaziana mafaili kama ilivyo elezwa hapo juu, lakini Piratebox ina waruhusu kufanya hivyo bila kujulikana, na pia hujumuisha vipengele vya kusogesha na kutuma meseji. Kuseti Piratebox ina hitaji upakue, usakinishe, na kuseti baadhi ya mifumo ya programu. [Maelekezo](#) yana patikana kwenye tovuti ya Piratebox.

Sasisha: mradi wa Pirate Box [unaelekea kuisha](#). Tovuti na eneo lao la kutunzia kumbukumbu mtandaoni vitaendelea kuwa mtandaoni, lakini mwanzilishi mkuu wa mradi hatakuwa akiendelea kuihudumia kikamilifu.

Wasiliana kupitia meseji za mtu kwa mtu

Aplikesheni mbili mpya za kutuma meseji za mtu kwa mtu ambazo tumezijua kupitia mitandao ya wanaharakati ni [Briar](#) na [Bridgefy](#). Applikesheni hizi sisi hatujazijaribu bado, lakini tunawajua wengine ambao wana zijaribu.

[Briar](#) ni aplikesheni ya meseji zilizosimbwa mwanzo hadi mwisho, na anayo weza mtu yeyote kutumia, ambayo haitegemei seva kuu, badala yake meseji zina sawazishwa baina ya simu za watumiaji (kwa hivyo maudhui yanakaa katika simu ya kila mtumiaji). Inaweza kusawazishwa hata wakati hamna mtandao kwa kutumia Bluetooth au WiFi (wakati kuna mtandao, aplikesheni husawazisha simu kutumia mtandao wa [Tor](#)). Briar pia huwa ina vipengele vya makundi binafsi, makongamano ya hadhara, na mablogu. Unapotumia bila mtandao, umbali unaoweza kufika unategemea Bluetooth au WiFi (ambapo vipimo vya juu kabisa huwa ni ~ mita 100).

Pia, [Bridgefy](#) ni aplikesheni ya kutuma meseji zilizo simbwa mwanzo hadi mwisho (isipokuwa wakati unatumia kipengele cha “kutangaza”) ambayo hutumia Bluetooth kutuma meseji. Kinyume na Briar, meseji zinaweza kwenda umbali mrefu zaidi kwa kupitia miundo ya mitandao ya watumiaji wengine wa Bridgefy (walengwa wa meseji pekee ndio wanaweza kuisoma). Bridgefy inakosa makundi binafsi, makongamano, na kipengele cha blogu kama Briar, lakini ina kuwezesha kutuma meseji hadi kwa watu saba wanatumia Bridgefy walio eneo husika kwa kutumia kipengele cha kutangaza, ambao hawahitaji kuwa kwenye namba zako za mawasiliano (Meseji za kutangaza sio lazima zisimbwe).

Kuwasiliana kupitia Meseji zilizosimbwa

Meseji hutumwa kupitia mitandao ya simu na haitegemei mtandao, kwa hiyo huendelea kufanya kazi hata wakati mtandao umezimwa. Hata hivyo, meseji zinaaminika kuwa hazina usalama. Kinyume na aplikesheni zinazo tegemea mtandao kama vile WhatsApp au Signal, meseji hazisimbwi moja kwa moja. Hii ina maanisha kwamba meseji (na maelezo yake) zinaweza kusomwa na serikali na mashirika ya simu, au kuingiliwa na matapeli wa mtandaoni. Meseji pia zinaweza “laghai,” kwa maana ya kwamba anayetuma meseji anaweza kutumia ujanja wa taarifa ya anwani yake na kujifanya mtumiaji mwingine.

Ikiwa unataka kutumia meseji, [Silence](#) ni aplikesheni ambayo husimba meseji mwanzo hadi mwisho. Ni aplikesheni iliyo huru kutumiwa na mtu yeyote, na hutumia utaratibu wa kusimba wa Signal. Wakati sisi wenyewe tukiwa hatujaijaribu, tumesikia kwamba wengine wameitumia. Kwa pamoja mtumaji na mpokeaji wote wanapaswa kusakinisha na kubadilishana neno la siri. Kwa vile meseji lazima zipite kwenye seva za makampuni ya huduma za mawasiliano, hata kwenye Silence japo unatuma meseji zilizosimbwa pamoja na taarifa zake, meseji hizo zinaweza kupekuliwa na makampuni ya huduma za mawasiliano.

Uzimaji kiasi wa mitandao: Suluhisho la tovuti zilizofungwa

“Kuzima mtandao” mara nyingi haimaanishi kukosekana kwa mtandao kabisa, ila ni kuzuia upatikanaji wa baadhi ya tovuti au mitandao ya kijamii. Serikali, kupitia watoa huduma za mtandao (ISPs), wanaweza kuzuia tovuti kulingana na anwani ya IP, maudhui, au kupitia taarifa za kwenye DNS. Hauna uhakika kama tovuti imezuliwa? Mashirika kama [Open Observatory of Network Interference](#) na [Netblocks](#) hufuatilia na kupima uvurugaji wa mtandao na ufuatiliaji ulimwenguni kote.

Kwa bahati nzuri, kwa kuwa unao mtandao, kuna baadhi ya njia unazoweza kujaribu ili kupata suluhisho la uzimaji kiasi wa mtandao. Kuhusu kusimba kumbuka kuwa kutafuta suluhisho la tovuti zilizofungwa kunaweza kuwa ni kosa la jinai katika nchi yako.

VPN

Njia mojawapo ya kukwepa kuzuiwa kwa IP na maudhui fulani ni kutumia mtandao binafsi wa kidigitali VPN, kama vile [ProtonVPN](#) au [TunnelBear](#). Unapo unganisha kupitia VPN, mtandao wako unafichwa na kuunganishwa kupitia seva ya VPN katika eneo jingine, kama vile katika nchi nyingine, hivyo kuficha sehemu ulipo kihalisia na maudhui yako katika mtandao unaotumia, ISP.

Kumbuka kwamba baadhi ya serikali zimepiga marufuku matumizi ya VPN au zinaweza kujaribu kuchunguza na kuzuia unganishwaji wa VPN. Ni muhimu pia kutumia watoaji wa VPN wanao aminika, na hasa wale ambao hawawezi kuhifadhi taarifa, kwani mtoaji huduma atakuwa anaona shughuli zako za mtandaoni. Kuwa makini na nchi anayotoka mtoaji wa VPN, na ni

sheria zipi zinazoweza kuwa wajibisha kutokana na nchi zao. Pia kumbuka VPN zilizo thibitishwa na serikali zinaweza kuwezesha taarifa zako kuchunguzwa na kukaguliwa.

Seva za DNS

Seva za DNS (“mfumo wa jina la kikoa”) hufanya kazi kwa kutafsiri majina ya kikoa au URL ambazo mtumiaji anaandika kwenye kivinjari hadi kwenye anwani za nambari za IP ambayo mtandao unatumia kutambua kurasa za tovuti. ISP inaweza kubadilisha seva za DNS inayodhibiti kuzuia baadhi ya maswali, au kurudisha kurasa isiyo sahihi inayo sema tovuti husika haipo. Mwaka 2014, Waziri Mkuu wa Uturuki Recep Tayyip Erdoğan [alijaribu kuzuia Twitter](#) wakati wa uchaguzi mkuu nchini humo akitumia mbinu hii. Kuzuiwa huko [kulitafutiwa mbadala kwa haraka](#) na wanaharakati ambapo walisambaza taarifa za hatua kwa hatua jinsi ya kutumia VPN na kubadilisha seva za DNS.

Unaweza kubadilisha seva msingi za DNS katika mtandao wa simu yako au mpangilio wa wifi. Badala ya seva msingi ya DNS, unaweza tumia seva mbadala za DNS kama [Google Public DNS](#).

Hizi ni njia mbili tu za kukwepa mbinu zilizo zoeleka sana katika kuzuia mitandao. Angalia miongozo muhimu ya kukusaidia kutoka [Internet Society](#), [Access Now](#), [Security-in-a-Box](#), na [EFF](#) kwa taarifa za kina zaidi.
