AYETA!

ZANA YA HAKI ZA KIDIJITALI

Kingdom of the Netherlands

PARADIGM INITIATIVE

Stanford PACS

AYETA

ZANA ZA HAKI ZA KIDIJITALI

Imechapishwa na Paradigm Initiative

Iliyochapishwa Aprili 2024

Watafiti:Khadijah El-Usman, Ihueze Nwobilor, Angela Onyegbuna, Bridgette Ndlovu, Miriam Wanjiru na Sani Suleiman
Wasaidizi wa utafiti: Dinchi Ikpa, Ifiokobong Uko na Joshua Oke
Imehaririwa na: Khadijah El-Usman na ‘Gbenga Sesan
Mhariri Mkuu: Izak Minnaar
La traduction de la langue:
Ubunifu na mpangilio:Kenneth Oyeniyi

UTANGULIZI

Wakati watetezi wa haki za kidijitali wanapoendelea kuwa na wasiwasi kuhusu usalama wao wa kidijitali, ni lazima wachukue hatua za kujikinga wanapotekeleza majukumu yao. Toleo hili jipya la zana ya Ayeta linajumuisha vidokezo na hatua za hivi karibuni za usalama wa kidijitali ili kujilinda dhidi ya vitisho vinavyoweza kutokea. Pia linajumuisha orodha za wadau wa usalama wa kidijitali, matukio muhimu ya haki za kidijitali barani Afrika, viungo vya tafiti za usalama wa kidijitali kutoka nchi kadhaa za Afrika, miundo ya maelezo ya sera, na ya taarifa za pamoja. Sehemu moja ya seti hii ya zana imefanyiwa kazi maalum kuhusu vizuizi katika mtandao, njia za kuzunguka vizuizi hivyo, jinsi ya kuhifadhi rekodi, na vifaa vya utetezi kwa matukio kama hayo.

Zana ya kwanza iliandaliwa kama sehemu ya mradi wa Ushirika wa Stanford wa mwaka 2020 wa Jamii ya Kidijitali. , Pamoja na msaada zaidi kutoka kwa Mfuko wa Haki za Binadamu wa Uholanzi. ‘Gbenga Sesan, akisaidiwa na Bonface Witaba, aliongoza uratibu wa mradi, maendeleo ya mtaala, uandishi, na uhariri, huku akipata msaada kutoka kwa timu ya Paradigm Initiative.

Tunashukuru washirika wa PIN ambao walitoa maoni juu ya jinsi ya kuboresha toleo lililopita, na maarifa yao muhimu yametusaidia kufanya zana hii kuwa bora zaidi kwa ulimwengu wa leo. Kulikuwa na jitihada kubwa zilizotumika katika utafiti na kuboresha zana hii, ambazo zilisimamiwa na wanachama wa timu ya PIN kama Angela Onyegbuna, Sani Suleiman, Khadijah El-Usman, Bridgette Ndlovu, Ihueze Nwobilor, Joshua Oke, na Miriam Wanjiru. Tunathamini kazi

1 https://pacscenter.stanford.edu/person/gbenga-sesan/

ya uhariri iliyofanywa na Izak Minnaar. Kazi ya utafiti iliongozwa na Judith Ogutu, Giyo Ndzi, na Samuel Ojezele wa PIN, huku Kenneth Oyeniyi na David Chima wakishughulikia masuala ya muundo. Dinchi Ikpa, Ifiokobong Uko, na Angela Onyegbuna wali rejesha upya viungo, na toleo hili la zana lilifanyiwa marekebisho na Khadijah El-Usman, Angela Onyegbuna, na ‘Gbenga Sesan.

Zana hii imeundwa kwa lengo kuu la kukidhi mahitaji yanayoongeza ya kulinda watetezi wa haki za kidijitali, waandishi wa habari, wafichuzi, na watu wengine wanaofanya kazi na taarifa nyeti katika maeneo ya nchi za Kusini duniani. PIN inaahidi kuhakikisha kwamba inabaki kuwa rasilimali inayoendelea kwa kuchapisha toleo zilizosasishwa. Tunategemea maoni yako ili kufanikisha hili - tafadhali tuma maoni, mawazo, ukosoaji, na hadithi kwa hello@ayeta.africa.

“Toleo hili jipya la zana ya Ayeta linajumuisha vidokezo na hatua za hivi karibuni za usalama wa kidijitali ili kujilinda dhidi ya vitisho vinavyoweza kutokea”

YALIYOMO

SURA 01 | HAKI ZA KIDIJITALI

Kuanzishwa kwa mtandao na kufunguliwa kwake kwa dunia mnamo mwaka 1989 kumeshuhudia watetezi wa haki za binadamu wakitumia ubunifu katika matumizi yao ya nafasi mtandaoni ili kusaidia kukuza uhuru wa kujieleza, uhuru wa kuungana mtandaoni, na kuongeza uwezo wa jamii ya kidijitali. Kwasasa, mtandao unaonekana kama faida kwa jamii, ukikutanisha zaidi ya nusu ya idadi ya watu duniani. Hata hivyo, umeanza kuwa hatari zaidi na kuna kuongezeka kwa matatizo yanayowakabili wanaharakati, watetezi wa haki za binadamu, wapinzani, na waandishi wa habari. Serikali zenye utawala wa kiimla zimeanza kutumia zana na mikakati ya kidijitali kama vile kuzima mtandao, kudhibiti mtandaoni, na upelelezi wa kidijitali kwa lengo la kudhibiti uhuru wa kujieleza.

Kama ilivyodhihirishwa katika Ripoti ya Paradigm Initiative kuhusu Haki za Kidijitali Barani Afrika ya mwaka 2019,[1] “Katika kipindi cha muongo uliopita, kumekuwa na kuongezeka kwa juhudi

1 https://paradigmhq.org/report/digital-rights-in-africa-2019

ya mashirika ya Kiafrika yanayopigania haki za kidijitali - kama vile upatikanaji wa mtandao wa bei nafuu na wa ubora, faragha, uhuru wa maoni, kujieleza na kuungana, miongoni mwa mambo mengine".Tofauti kabisa na hali hii ya kuibuka upya kwa haki za kidijitali miongoni mwa raia katika bara hilo, maono ya serikali za Kiafrika kuhusu jukumu la uunganishaji wa mtandao na upatikanaji wa kidijitali barani kwa kiasi kikubwa kimekuwa ni kuhusu kudumisha madaraka ya kisiasa na udhibiti kwa njia zote. Hisia kuu imekuwa kwa kiasi kikubwa kuweka haki na upatikanaji chini ili kudumisha udhibiti wa kisiasa juu ya raia." Ripoti ya Haki za Kidijitali na Ujumuishi Barani Afrika ya Londa ya mwaka 2022[2] inaonyesha masuala mapya yanayojitokeza: "Teknolojia mpya kama vile Akili Mnemba (AI) inazidi kupata umaarufu, uelewa, na kukubalika katika bara la Afrika." vilevile "usiri na utawala wa data pamoja na ukosefu wa uwajibikaji na usimamizi."

Ripoti ya 2022 kutoka Access Now ilionyesha idadi kubwa zaidi ya kuzimwa kwa mtandao katika kipindi cha mwaka mmoja: Mtandao ulizimwa katika nchi 35 kote duniani. Kati ya hizo, saba zilikuwa barani Afrika. (Burkina Faso, Ethiopia, Sierra Leone, Nigeria, Somaliland, Uganda, and Zimbabwe). Kwa kuzingatia, mwaka uliopita kulikuwa na kuzimwa kwa mtandao katika nchi 12 za Afrika.[3]

Hatua za nchi hizi zinaenda kinyume moja kwa moja na Kanuni ya 38.2. (*"Mataifa hayapaswi kushiriki au kuweka kizuizi chochote cha ufikiaji wa mtandao na teknolojia nyingine za kidijitali kwa umma au kwa nchi nzima."*) kutoka kwa Azimio la Mwaka wa 2019 kuhusu Misingi ya Uhuru wa Kujieleza na Upatikanaji wa Habari Barani Afrika.[4] iliyotolewa na Tume ya Afrika kuhusu Haki za Binadamu na Watu (Azimio la 2019 la ACHPR), pamoja na Azimio la pamoja la Umoja wa Mataifa la Haki za Binadamu.[5]

2.1.

Haki za Kidijitali ni nini?

Haki za kidijitali ni msingi wa haki za binadamu katika zama hizi za kimtandao. Kwa mfano, haki za faragha mtandaoni na uhuru wa kujieleza ni upanuzi wa haki sawa na zisizoweza kuchukuliwa zilizoelezwa katika Azimio la pamoja la Haki za Binadamu la Umoja wa Mataifa.[6] Haki za kidijitali zinahusu haki za watu kupata kompyuta na uwezo wa kutumia na kuchapisha maudhui ya kidijitali. Hii ina maana inahusu ruhusa zinazoruhusiwa kwa matumizi ya haki ya vifaa vya kidijitali na haki ya faragha. Kulingana na Umoja wa Mataifa, kumkatia mtu mtandao kunakiuka haki hizi na ni kinyume cha sheria za kimataifa.[7]

Pamoja na hayo, kifungu cha utangulizi cha Azimio la 2019 la ACHPR kina thibitisha kwamba haki sawa zinazopatikana nje ya mtandao zinapaswa kulindwa vivyo hivyo mtandaoni, na kinatambua umuhimu wa kutumia mtandao

2 https://paradigmhq.org/wp-content/uploads/2023/04/Londa-2022.pdf
3 https://www.accessnow.org/wp-content/uploads/2023/03/2022-KIO-Report-Africa.pdf
4 https://achpr.au.int/en/node/902
5 https://www.un.org/en/about-us/universal-declaration-of-human-rights
6 https://www.un.org/en/about-us/universal-declaration-of-human-rights
7 https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

kwa uhuru wa kujieleza na kupata habari katika kufurahia haki zingine na kupunguza pengo la kidijitali.[8] - kutekeleza kwa ufanisi haki za kupata habari na uhuru wa kujieleza kama ilivyo ainishwa katika Kifungu cha 9 cha Mkataba wa Afrika kuhusu Haki za Binadamu na Watu ili ziweze kuwa na mafanikio mazuri katika zama hizi za kidijitali.

1.2.

Nyaraka za Haki za Kidijitali/Binadamu, Tamko, Itifaki, na Mikataba

Haki za binadamu zinazotumika katika mahusiano yote ya binadamu, iwe mtandaoni au nje ya mtandao, kama ilivyo elezwa hapo awali. Misingi iliyo ainishwa katika haki za kidijitali na haki za binadamu kwa ujumla inapaswa kuhusishwa ili kutumika katika mazingira ya mtandao na maeneo yote ya kutunga sera za mtandao.

Azimio la Haki za Binadamu la Umoja wa Mataifa[9]

Azimio la Haki za Binadamu la Umoja wa Mataifa (UDHR) ni hati muhimu katika historia ya haki za binadamu. Lililowekwa na wawakilishi wenye asili tofauti kisheria na utamaduni kutoka kila kona ya dunia, Azimio hilo lilitangazwa na Baraza Kuu la Umoja wa Mataifa huko Paris mnamo tarehe 10 Disemba 1948 (Azimio la Baraza Kuu la Umoja wa Mataifa 217 A) kama kiwango cha maafikiano ya pamoja kwa watu wote na mataifa yote.Inabainisha haki za msingi za binadamu ambazo zinapaswa kulindwa kote duniani na imetafsiriwa katika lugha zaidi ya 500.

Azimio la Haki za Binadamu na Watu Barani Afrika[10]

Azimio la Banjul, au Mkataba wa Afrika kuhusu Haki za Binadamu na Watu, ni chombo cha haki za binadamu kinacholenga kukuza na kulinda haki za binadamu na uhuru wa msingi barani Afrika. Azimio hilo lilipitishwa tarehe 1 Juni 1981, likaanza kutumika rasmi tarehe 21 Oktoba 1986, na bado ni chombo muhimu cha haki za binadamu cha Umoja wa Afrika (AU). Azimio hilo lilianzisha Tume ya Afrika kuhusu Haki za Binadamu na Watu ili kusimamia utekelezaji wa haki za kibinafsi, kijamii-kiuchumi, kiraia, na kisiasa zilizojumuishwa katika mkataba huo.[11]

Mkataba wa Malabo[12]

Mkataba wa Umoja wa Afrika kuhusu Usalama wa Mtandao na Ulinzi wa Data za Kibinafsi, ambao unajulikana kama Mkataba wa Malabo, ni makubaliano ya kisheria yanayobana kuhusu ulinzi wa data katika eneo la kikanda, na ni tofauti na Ulaya. Ilipata nguvu tarehe 8 Juni 2023 baada ya kuridhiwa na nchi 15, miaka tisa baada ya kupitishwa kwake tarehe 27 Juni

8 https://achpr.au.int/en/node/902
9 https://www.un.org/en/about-us/universal-declaration-of-human-rights
10 https://au.int/en/treaties/african-charter-human-and-peoples-rights
11 https://achpr.au.int/en
12 https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

2014. Mkataba huo unatoa mfumo kamili wa bara zima wa kuboresha sera za ulinzi wa data, haki za kidijitali, faragha, na uhuru wa mtandao. Mkataba wa Malabo unalenga, pamoja na mambo mengine, kutimiza malengo mawili makuu. Kwanza, unazitaka nchi wanachama kuanzisha mfumo wa kisheria unaofaa wa kulinda haki za msingi na data za kibinafsi. Pili, unalenga kusawazisha haki za msingi za wamiliki wa data na mamlaka ya serikali pamoja na haki za jamii za ndani.[13]

Azimio la ACHPR la Kanuni za Uhuru wa Kujieleza na Upatikanaji wa Habari Barani Afrika[14]

Azimio la ACHPR la 2019 linachukua nafasi ya Azimio la 2002 kuhusu Uhuru wa Kujieleza Afrika, likiwa na sehemu mpya zinazohusu upatikanaji wa taarifa na haki za mtandaoni. Linazingatia viwango vya sheria ngumu na laini vilivyotolewa kutoka kwa vyombo vya haki za binadamu vya Afrika na kimataifa, pamoja na hukumu za vyombo vya mahakama vya Afrika. Azimio hili lina kanuni kuhusu wajibu wa nchi kulinda haki za mtandaoni, kuhakikisha upatikanaji wa mtandao wa kijumla, wa haki, wa bei nafuu, na wa maana, ulinzi wa taarifa za kibinafsi mtandaoni, na ufuatiliaji wa mawasiliano.

Muundo wa Sera ya Data wa Umoja wa Afrika[15]

Muundo wa Sera ya Takwimu ya Umoja wa Afrika (DPF), uliochapishwa mwezi Julai 2022, ni mojawapo ya nyaraka muhimu sana za utawala wa takwimu katika bara la Afrika. Kilichoundwa na Tume ya Umoja wa Afrika kwa ushirikiano na washirika ndani na nje ya mfumo wa AU, Mfumo wa Sera ya Takwimu (DPF) ulipitishwa na Baraza la Utekelezaji la AU mwezi Februari 2022. DPF ni mwongozo wa kina unaolenga kusaidia juhudi za nchi za Afrika katika kuweka mifumo madhubuti ya utawala wa takwimu ili kufaidika na mageuzi ya data na kidijitali yanayoendelea. Ingawa kama vyombo vingi vya sera za kikanda na kimataifa, DPF haina nguvu za kisheria kwa nchi wanachama wa AU, ni rasilimali muhimu kwa serikali na wadau wa mapinduzi ya data barani Afrika.[16]

Azimio la Haki na Uhuru wa Mtandao Barani Afrika[17]

Azimio la Afrika kuhusu Haki na Uhuru wa Mtandao (AfDec) ni harakati za pamoja za muungano wa kijamii wa Kiafrika kusukuma viwango vya haki za binadamu na kanuni za uwazi katika uundaji na utekelezaji wa sera za mtandao barani. Lengo la AfDec ni kuongeza maelezo kuhusu kanuni zinazohitajika

13 https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/
14 https://achpr.au.int/en/node/902
15 https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf
16 https://cipesa.org/wp-content/files/briefs/Five_Takeaways_From_the_2022_African_Union_Data_Policy_Framework_Brief.pdf
17 https://africaninternetrights.org/about/

kudumisha haki za binadamu na watu kwenye mtandao, na kukuza mazingira ya mtandao yanayoweza kukidhi mahitaji na malengo ya maendeleo ya kijamii na kiuchumi ya Afrika. AfDec inategemea nyaraka za haki za binadamu za Kiafrika zilizowekwa vizuri, kama vile Azimio la Haki na Haki za Watu wa Kiafrika na Azimio la Windhoek kuhusu Kuhamasisha Vyombo vya Habari Visivyoegemea na Vyombo vya Habari Vilivyodumishwa.[18] Mkataba wa Afrika wa Utangazaji wa mwaka 1991[19] la mwaka 2001, Azimio la awali la Kanuni za Uhuru wa Kujieleza Barani Afrika la 2002 na Jukwaa la Afrika la Upatikanaji wa Taarifa.[20] la mwaka 2011.

Azimio la Umoja wa Afrika kuhusu Usimamizi wa Mtandao.[21] Azimio la Umoja wa Afrika kuhusu Usimamizi wa Mtandao la mwaka 2017 lilipitishwa kupitia mchakato wa mashauriano na lengo la kutumia faida za uchumi wa kidijitali ili kuunda mazingira yanayofaa kwa wadau wa Kiafrika kujadili masuala muhimu yanayoibuka na kuchangia katika maendeleo ya sera za umma za mtandao ambazo zinazingatia mahitaji ya Afrika. Tamko hilo linawakilisha kanuni za mwongozo kwa wadau na linajumuisha thamani zinazo shirikishwa katika majadiliano kuhusu mustakabali wa mtandao kutoka mtazamo wa Kiafrika.

1.3.

Mikataba ya Kikanda

Afrika ina mashirika mbalimbali ya kikanda, ambayo mara nyingi huitwa Jumuiya za Kiuchumi za Kikanda (RECs) - hizi ni Jumuiya ya Maendeleo ya Kusini mwa Afrika (SADC), Mamlaka ya Maendeleo ya Serikali Kuu (IGAD), Jumuiya ya Kiuchumi ya Nchi za Afrika ya Kati (ECCAS), Umoja wa Maghreb Arabu (AMU), Jumuiya ya Nchi za Sahel-Sahara (CEN-SAD), Soko la Pamoja la Afrika Mashariki na Kusini (COMESA), Jumuiya ya Afrika Mashariki (EAC), na Jumuiya ya Kiuchumi ya Nchi za Afrika Magharibi (ECOWAS). Baadhi ya jumuiya hizi zina mikataba yao wenyewe kama vile Sera ya ECOWAS ya Ulinzi wa Miundombinu Muhimu ya Kikanda.[22] na Mwongozo wa ECOWAS wa Uhalifu wa Mtandao (uliopitishwa mwaka 2011), na Mfumo wa Sera ya Mawasiliano ya Mtandao na Tehama wa Jumuiya ya Afrika ya Mashariki,[23] Na SADC ina Sheria ya muundo wa Jinai wa Kompyuta na Uhalifu wa Mtandaoni. (2012).[24]

1.4.

Sheria za Nchi

Kiwango cha hali ya sheria hizi, maazimio na mikataba hutekelezwa na sheria za haki za binadamu, sheria za kitaifa za ulinzi wa data na mara nyingi sheria za uhalifu wa mtandao.

18 https://www.veritaszim.net/sites/veritas_d/files/Windhoek-Declaration%281%29.pdf
19 http://www.mediaombudsmannamibia.org/pdf/African_Charter_on_Broadcasting.pdf
20 https://www.africanplatform.org/fileadmin/Content/PDF/APAI-Declaration-English.pdf
21 https://au.int/sites/default/files/newsevents/workingdocuments/33025-wd-african_declaration_on_internet_governance_en_0.pdf
22 https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Critical-Infrastructure-Protection-Policy-EN.pdf
23 https://eaco.int/admin/docs/publications/EAC_MODEL_ICT_POLICY.pdf
24 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf

Kwa mujibu wa taarifa iliyochapishwa na Data Protection Africa, ifikapo Januari 2024, nchi 35 barani Afrika zilikuwa zimepitisha sheria za kitaifa za ulinzi wa data na nchi tatu zilikuwa zimeandaa miswada ya sheria kuhusu ulinzi wa data.[25]

25 https://dataprotection.africa/

1.5.

Wadau wa Usalama wa Kidijitali

Wadau wengi wa usalama wa kidijitali wana mipango ya kupunguza madhara na hatari kwa waandishi wa habari na walinzi wa haki za binadamu. Mashirika haya yanaweza kuwasiliana kwa ushauri na/au msaada kuhusu masuala yanayohusiana na uvunjaji wa data, ripoti za matukio, masuala ya sera, n.k.

AccessNow[26]

AccessNow inatoa huduma ya simu ya dharura ya usalama wa kidijitali saa nane kwa siku, uchambuzi wa sera kwa kutegemea ushahidi, utetezi, na ruzuku kwa mashirika ya msingi na vikundi vya wanaharakati vinavyofanya kazi na watumiaji na jamii ambazo ziko hatarini zaidi kwa uvunjaji wa haki za kidijitali.

AfricanDefenders[27]

Mtandao wa wanaharakati wa haki za binadamu barani Afrika kutoka mashirika matano ya kikanda ya Kiafrika[28] Unaohusika na kukuza na kulinda walinzi wa haki za binadamu (HRDs) katika bara la Afrika.

Kitovu cha Haki za Kidijitali Afrika (ADRH)[29]

Kitovu cha Haki za Kidijitali Afrika (ADRH) ni taasisi isiyo tengeneza faida inayofanya kazi kama “kituo cha kufikiria na kutekeleza,” ambayo inakuza utafiti na ujenzi wa uwezo wa pana kuhusu haki za kidijitali barani Afrika. Kwa kuzingatia jinsi teknolojia ya kidijitali inavyowaathiri watu, Kitovu cha Haki za Kidijitali Afrika (ADRH) inakusanya watafiti wa taaluma, wadau mbalimbali, watunga sera, na mashirika ya kikanda na kimataifa ili kushughulikia masuala ya haki za kidijitali barani Afrika.

26 https://www.accessnow.org/
27 https://africandefenders.org/
28 https://africandefenders.org/members/
29 https://africadigitalrightshub.org/

Mtandao wa Haki za Kidijitali Afrika (ADRN)[30]

Huu ni mtandao wa wanaharakati, wasomi, na wachambuzi ambao wanafanya utafiti kuhusu haki za kidijitali katika Afrika. Wanafanya utafiti wa kipekee, wanatoa ripoti za kipekee, na wanachapisha mfululizo wa vitabu vya kisasa kuhusu haki za kidijitali.

Mtandao wa Africtivists[31]

Mtandao wa Pan-Afrika wa wanaharakati na wablogu mtandaoni kwa ajili ya demokrasia, ukiwa na jamii ya wanaharakati wa kidijitali 200 kutoka nchi 35 mbalimbali.

Chama cha Mawasiliano ya Maendeleo (APC)[32]

APC inajitahidi kujenga dunia ambayo watu wote wanaweza kupata kwa urahisi, kwa usawa na kwa gharama nafuu fursa za ICT ili kuboresha maisha yao na kuunda jamii zenye demokrasia na usawa zaidi.

Chama cha Wanawake Wanahabari nchini Kenya (AMWIK)[33]

AMWIK ni chama cha kitaifa cha wanahabari kilichojikita katika kuongeza uwakilishi wa wanawake katika jamii na kuchochea ushiriki wao katika uongozi na maamuzi.

Chama cha Mawakili wa Faragha barani Afrika (APLA)[34]

APLA ni shirika la uanachama lililoanzishwa mwaka 2022 lenye lengo la kusaidia juhudi za pamoja katika kutambua, kuendeleza na kuboresha taaluma ya sheria ya faragha ya data katika nchi zote za Afrika.

30 https://www.africandigitalrightsnetwork.org/
31 https://www.africtivistes.org/
32 https://www.apc.org/
33 http://amwik.org/
34 https://aplafrica.com/

Shirika la Article 19[35]

Article 19 inalenga kuwawezesha watu kote duniani kujieleza kwa uhuru na kushiriki kikamilifu katika maisha ya umma bila hofu ya kubaguliwa.

Shirika la CoCreation Hub Nigeria[36]

Huitwa kwa kifupi Cc-HUB au HUB, ni jukwaa ambapo watu wenye maslahi katika teknolojia wanashirikiana kubadilishana mawazo kuhusu jinsi ya kutatua matatizo ya kijamii nchini Nigeria na mahali pengine.

Ushirikiano wa Sera za Kimataifa za Teknolojia ya Habari na Mawasiliano kwa Kanda ya Afrika Mashariki na Kusini (CIPESA)[37]

Shirika la CIPESA, lenye makao yake jijini Kampala, Uganda, ni shirika linalo husika na sera za mtandao linalopigania sera na matumizi ya TEHAMA yenye tija na pana kwa lengo la kuboresha utawala, maisha ya watu, na haki za binadamu barani Afrika.

Kamati ya Kulinda Waandishi wa Habari (CPJ)[38]

Shirika lisilo la faida, lisilo la serikali, lenye makao yake jijini New York na waandishi wa habari katika maeneo mbalimbali duniani. CPJ linapigania uhuru wa vyombo vya habari na kulinda haki za waandishi wa habari ulimwenguni.

Shirika la Usalama wa Mtandao Afrika[39]

Kampuni ya ushauri wa usalama wa taarifa inayotoa mbalimbali ya huduma na bidhaa ili kusaidia mashirika kulinda mali zao muhimu.

35 https://www.article19.org/
36 https://cchub.africa
37 https://cipesa.org/
38 https://cpj.org/
39 https://www.cybersecurityafrica.com/

Muungano wa Watetezi, Kenya[40]

Muungano wa kitaifa nchini Kenya unalenga kuongeza uwezo wa watetezi wa haki za binadamu ili waweze kufanya kazi kwa ufanisi na kupunguza hatari ya kuteswa, pamoja na kusukuma mazingira mazuri kisheria na kisera.

Jamii ya Kidijitali ya Afrika (DSA)[41]

DSA inafanya kazi ya kuimarisha uthabiti na uwezo wa wanaharakati kuwa mstari wa mbele, watetezi wa haki za binadamu na makundi mengine hatarishi katika eneo hilo kutambua na kukabiliana na vitisho na mashambulizi ya kidijitali kwa uhuru.

Muungano wa Usalama wa Kidijitali (DSA)[42]

Muungano wa mashirika na wataalamu binafsi wa usalama wa kidijitali nchini Uganda unaofanya kazi ya kulinda mali za kidijitali za jamii za kiraia, watetezi wa haki za binadamu, waandishi wa habari na wanaharakati wengine dhidi ya vitisho kutoka kwa makampuni yenye nguvu, wahalifu wasio na maadili, serikali na wahusika wengine wasio serikali.

Shirika la Freedom House[43]

Shirika lisilo la faida na lisilo la serikali lenye makao yake Marekani, linalojihusisha na utafiti na utetezi kuhusu demokrasia, uhuru wa kisiasa, na haki za binadamu.

40 https://defenderscoalition.org/
41 https://digitalsociety.africa/
42 https://www.defendersprotection.org/dsa/
43 https://freedomhouse.org/

Shirika la Frontline Defenders[44]

Shirika la haki za binadamu lililoanzishwa Dublin, Ireland mwaka 2001 kwa lengo la kulinda wale wanaofanya kazi kwa amani kusimamia haki za binadamu kama zilivyoelezwa katika Azimio la Pamoja la Haki za Binadamu.

Muungano wa Usalama wa Kidijitali Gambia[45]

Shirika linalenga kuongeza ufahamu na kuelewa zaidi kwa Wagambia kuhusu usalama wa mtandao, vitisho vya mtandao, upelelezi, na kuwapa uwezo wa kuwa salama na imara zaidi mtandaoni.

Chama cha Waandishi wa Habari Gambia[46]

Chama cha Waandishi wa Habari Gambia ni umoja wa wafanyakazi wa habari nchini Gambia, kilichoundwa mwaka 1978 na kikundi cha waandishi wa habari, kwa lengo la kukuza vyombo vya habari huru na vyenye nguvu.

Mtandao wa Watetezi wa Haki za Binadamu - Sierra Leone (HRDN-SL)[47]

Mtandao wa Watetezi wa Haki za Binadamu - Sierra Leone (HRDN-SL) ni muungano wa mashirika ya kiraia ya haki za binadamu na watu binafsi wanaofanya kazi kwa ajili ya ulinzi na uhamasishaji wa haki za binadamu nchini Sierra Leone.

Mtandao wa Teknolojia ya Habari, Mawasiliano (TEHAMA) Kenya (KICTANET)[48]

Ni jukwaa la wadau TEHAMA (ICT) lenye kuratibu mawazo kutoka kwa wadau mbalimbali wanaopenda na kushiriki katika sera na udhibiti wa Teknolojia,

44 https://www.frontlinedefenders.org/
45 https://twitter.com/CyberGambia
46 https://gpu.gm/
47 https://grassrootsjusticenetwork.org/connect/organization/pan-african-human-rights-defenders-network/
48 https://www.kictanet.or.ke

Habari na Mawasiliano (ICT). Kazi yake inaongozwa na nguzo nne: ushawishi wa sera, kuimarisha uwezo, utafiti, na ushirikiano na wadau.

Shirika la Media Foundation for West Africa (MFWA)[49]

Ulianzishwa mwaka 1997 na makao yake Accra, Ghana, MFWA ni shirika lisilo la kiserikali la kikanda linalosimamia na kulinda haki ya uhuru wa kujieleza kwa watu wote, hususan vyombo vya habari na watetezi wa haki za binadamu katika Afrika Magharibi.

Shirika la Media Defence (Ulinzi wa Vyombo vya Habari)[50]

Shirika lisilo la kiserikali lililoanzishwa mwaka 2008 kwa lengo la kutoa msaada wa kisheria kwa waandishi wa habari na vyombo vya habari huru. Pia linasaidia mafunzo katika sheria za vyombo vya habari na kukuza kubadilishana taarifa, zana za kushtaki na mikakati kwa mawakili wanaoshughulikia kesi za uhuru wa vyombo vya habari.

Shirika la Paradigm Initiative (PIN)[51]

PIN ni shirika ya kijamii inayojenga mfumo wa msaada ulioimarishwa na TEHAMA na kutetea haki za kidijitali ili kuboresha maisha ya vijana wasio na huduma ipasavyo. Mpango wa utetezi wa haki za kidijitali wa PIN unazingatia maendeleo ya sera za umma kwa uhuru wa mtandao barani Afrika.

Shirika la PeaceWomen[52]

Programu ya Wanawake, Amani na Usalama ya Shirikisho la Kimataifa la Wanawake kwa Amani na Uhuru (WILPF)[53], shirika la kimataifa linalojenga amani kwa msingi wa kifeministi.

49 https://www.mfwa.org/
50 https://www.mediadefence.org/
51 https://paradigmhq.org/
52 https://www.peacewomen.org/
53 http://wilpf.org/

Shirika la Pollicy[54]

Kikundi cha kifeministi cha wataalam wa teknolojia, wanasayansi wa data, watu wa ubunifu na watafiti wanaofanya kazi katika ugo wa data, ubunifu na teknolojia ili kuboresha uzoefu wa maisha kwa kushawishi utamaduni wa matumizi sahihi ya data, kuendeleza mazoea mazuri ya usimamizi wa data, na kutetea sera zinazounga mkono mfumo wa data unaowezesha.

Shirika la Safe Sisters[55]

Safe Sisters ni programu ya ushirika kwa wanaharakati wa haki za binadamu wanawake, waandishi wa habari, wafanyakazi wa vyombo vya habari, na wanaharakati. Washiriki wanapata mafunzo ya kuelewa na kukabiliana na changamoto za usalama wa kidijitali wanazokutana nazo katika kazi zao na maisha ya kila siku.

Shirika la Women of Uganda Network (WOUGNET)[56]

WOUGNET inahamasisha matumizi ya teknolojia ya habari na mawasiliano kati ya wanawake na wasichana kama zana za kushirikiana habari na kushughulikia masuala kama usawa wa kijinsia na maendeleo endelevu.

Taasisi ya Zambian Cyber Security Initiative Foundation[57]

ZCSI ni taasisi ya Ulinzi wa Mtandao ya Zambia inayotoa elimu na vifaa vya ulinzi na usalama katika ulimwengu wa kidijitali wa leo na kulinda watu binafsi na mashirika kutokana na madhara ya vitisho vya mtandao.

54 https://pollicy.org/
55 https://safesisters.net/
56 https://wougnet.org
57 https://zcsi-foundation.org/

1.6.

Matukio ya Haki za Kidijitali

Kila mwaka, barani Afrika, kuna matukio kadhaa ya haki za kidijitali na usalama yanayoandaliwa, yakileta pamoja wadau kutoka maeneo mbalimbali kujadili masuala ya sera, mwelekeo mpya na kutoa mafunzo ya vitendo.

Shule ya Utawala wa Mtandao ya Afrika (AfriSIG)[58]

Mpango wa mafunzo kwa wadau mbalimbali unaolenga kuwapa Waafrika fursa ya kupata maarifa na ujasiri wa kushiriki kikamilifu katika mchakato na mijadala ya utawala wa mtandao kwenye ngazi ya kitaifa, kikanda na kimataifa.

Shule nyingine za utawala wa mtandao kwenye ngazi za kikanda na kitaifa ni pamoja na:

- Shule ya Utawala wa Mtandao wa Afrika Magharibi (WASIG)[59]
- Shule ya Utawala wa Mtandao ya Kenya (KeSIG)[60]
- Shule ya Utawala wa Mtandao ya Nigeria (NSIG)[61]
- Shule ya Utawala wa Mtandao ya Sudan Kusini (SSSIG)[62]
- Shule ya Utawala wa Mtandao kwa Wanawake Arusha (AruWSIG)[63]

Jukwaa la Kidijitali na Ushirikishwaji wa Haki (DRIF)[64]

DRIF ni jukwaa linalofanyika kila Aprili na Paradigm Initiative ambapo masuala magumu na ya kimataifa kuhusu haki za mtandao, hasa barani Afrika, hujadiliwa kati ya jamii za kiraia, makampuni ya teknolojia, serikali, vyuo vikuu, na wadau wengine.

Jukwaa la Uhuru wa Mtandao Barani Afrika (FIFAfrica)[65]

Huandaliwa kila mwaka mwezi Septemba na CIPESA,[66] FIFAfrica inazingatia kukuza mtandao huru na wazi barani Afrika.

58 https://afrisig.org/
59 https://waigf.org/about-wasig/
60 https://kigf.or.ke/kesig/
61 https://sig.ng/
62 https://ssigf.org.ss/about-ss-sig/
63 https://www.ksgen.or.tz/aruwsig/
64 https://drif.paradigmhq.org/
65 https://internetfreedom.africa/
66 https://cipesa.org/service/forum-on-internet-freedom-in-africa/

1.7.

Mifano ya Kesi za Haki za Kidijitali

Juhudi za serikali za kukiuka haki za waandishi wa habari na watetezi wa haki za kidijitali kupitia sheria, kufunga mtandao na hatua za mahakama, pamoja na njia nyingine, zimeonyeshwa na mifano ifuatayo katika maeneo mbalimbali barani Afrika:

Kameruni: Nchini humo, ni changamoto kwa chombo cha habari kuendeleza sera ya uhariri huru na ya ukosoaji bila kukabiliwa na vitisho na usumbufu mkubwa iwapo taarifa zao zitahatarisha maslahi ya serikali na viongozi wake.Mazingira ya ukandamizaji huchochea waandishi wa habari kujizuia na kusababisha vyombo vingi vya habari kufuata maoni ya mamlaka au watu wenye ushawishi karibu nao. Waandishi wa habari wa Kameruni, hasa wale wanaosisitiza au kutoa maoni yao kwa uwazi, daima wanakabiliwa na hatari ya mashambulizi ya maneno au ya kimwili. Kwa mfano, mwili uliopatikana ukiwa umeharibiwa vibaya wa mwandishi wa habari Martinez Zogo ulipatikana baada ya siku tano tangu alipotekwa nyara mwezi Januari 2023.[67] Kama mtangazaji wa kipindi maarufu cha redio cha kila siku cha Embouteillage (au Gridlock kwa Kiingereza), mara kwa mara akizungumzia kesi za rushwa na madai ya ubadhirifu bila kusita kutaja majina ya watu mashuhuri. Mauaji ya Martinez Zogo yaliacha watu wengi wakishangazwa huku mashirika yasiyo ya kiserikali yakiongoza kulaani ukiukwaji wa uhuru wa vyombo vya habari na uhuru wa kujieleza.[68]

Misri: Tarehe 22 Agosti 2023, vikosi vya usalama vya serikali vilivyovalia kiraia vilimkamata Gamal Abdelhamid Ziada, baba wa mwandishi huru wa Misri Ahmed Gamal Ziada ambaye anaishi Ubelgiji, kwenye viunga vya mji wa Giza, kulingana na taarifa za habari na ujumbe wa Twitter kutoka kwa mwandishi huyo.[69] Siku iliyofuata, waendesha mashtaka walimfungulia mashtaka baba yake, Gamal Ziada, kwa matumizi mabaya ya mitandao ya kijamii, kusambaza habari za uongo na kuwa mwanachama wa kundi lililopigwa marufuku, na wakaamuru azuiliwe hadi kesi yake itakapofanyika. Ahمed Gamal Ziada anazungumzia masuala ya haki za binadamu na sera za nje za Misri kupitia tovuti huru za habari za kikanda kama vile Raseef, Daraj na Middle East Eye.[70] Serikali ya Misri iliendelea kuwanyamazisha wakosoaji kwa kuwakamatwa na kuwafungulia mashtaka yasiyo haki waandishi wa habari na wanablogu, huku bunge likipitisha sheria kali zaidi zinazozuia uhuru wa kujieleza na upatikanaji wa habari. Mbali na kutumia mahakama za usalama wa serikali, ambako hukumu haziwezi kukatiwa rufaa, mamlaka zinaendelea kuwashtaki maelfu ya raia katika mahakama za kijeshi. Mfumo wa mahakama zote mbili unajulikana kwa ukatili na haukidhi viwango vya msingi vya mchakato wa

67 https://rsf.org/en/country/cameroon
68 Cameroonian prosecutors wind up probe into the murder of Martinez Zogo I Africanews
69 إعتقال والد الناشط المصري أحمد جمال زيادة
70 https://cpj.org/2023/08/egyptian-authorities-arrest-father-of-freelance-journalist-ahmed-gamal-ziada/

haki, kwa mujibu wa Ripoti ya Dunia ya Human Rights Watch ya mwaka 2019.[71]

Nigeria: Teknolojia ya ufuatiliaji imekuwa ikitumiwa kupeleleza wanaharakati wa amani, wanasiasa wa upinzani na waandishi wa habari, na kuwalenga kwa unyanyasaji, kukamatwa na kuteswa, kinyume na sheria za kimataifa za haki za binadamu na hatua za kujidhibiti za makampuni yanayotoa huduma hizo. Nigeria ni moja ya wateja wakuu wa teknolojia zote kubwa za ufuatiliaji, ikijumuisha ufuatiliaji wa mtandao na simu, ufuatiliaji wa mitandao ya kijamii, data za utambulisho wa kibaiometriki na ufuatiliaji wa “mji salama” wa wananchi katika maeneo ya umma. Kwa mfano, Omoyele Sowore, mwanaharakati wa haki za binadamu na mgombea wa zamani wa urais, aligundua kuwa serikali ya Nigeria ilikuwa imezima kitambulisho chake cha kibaiometriki mnamo Januari 2022. Hii ilimaanisha kuwa kadi yake ya kitaifa ya utambulisho, kadi ya kudumu ya mpiga kura, pasipoti ya kigeni na leseni ya udereva vilikuwa miongoni mwa nyaraka zilizozimwa, na hivyo kumzuia kusafiri, kuendesha gari au kupiga kura.[72]

Tanzania: Kulingana na ripoti ya Idara ya Jimbo la Marekani kuhusu haki za binadamu[73] ya mwaka 2022, tarehe 27 Juni 2022, serikali ilimwandikia barua DarMpya Media ikidai kuwa ilipotosha maandamano ya tarehe 17 Juni nje ya Ubalozi wa Kenya mjini Dar es Salaam, kuhusu mvutano kati ya wakazi wa Kimasai na mamlaka huko Loliondo. Serikali ilidai DarMpya ilikuwa ikifanya kazi bila leseni na ikapiga marufuku chombo hicho kuchapisha maudhui mtandaoni. DarMpya iliomba upya leseni yake ya uchapishaji mnamo Agosti mwaka huo, lakini ombi hilo lilikataliwa na Mamlaka ya Mawasiliano Tanzania. (TCRA).

Uganda: Serikali ya Uganda ilifunga huduma ya intaneti na majukwaa ya mitandao ya kijamii wakati wa uchaguzi wa urais na bunge mwezi Januari 2021, ikizuia mawasiliano na fursa ya kupata habari.[74] Takwimu za mtandao kutoka NetBlocks Internet Observatory zinaonyesha kwamba kuna vizuizi vya kina kwenye mitandao ya kijamii na majukwaa ya mawasiliano mtandaoni kwa watoa huduma wakubwa wa mtandao nchini Uganda tangu Jumanne, tarehe 12 Januari, siku mbili kabla ya uchaguzi. Uchunguzi wa NetBlocks unaonesha jinsi vizuizi hivyo vimeamriwa na mamlaka.[75] ya Tume ya Mawasiliano ya Uganda kabla ya uchaguzi tarehe 14.[76] Kizuizi kiliondolewa siku ya Jumatatu baada ya uchaguzi, zaidi ya masaa 100 baada ya kuwekwa. Mamlaka zilisikitishwa na usumbufu uliotokea na kusema kuwa kufungwa kulilenga kuzuia kuingiliwa

71 https://www.hrw.org/world-report/2019/country-chapters/egypt
72 https://www.ids.ac.uk/press-releases/nigeria-spending-billions-of-dollars-on-harmful-surveillance-of-citizens/
73 https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/tanzania/
74 https://www.hrw.org/world-report/2022/country-chapters/uganda
75 https://www.reuters.com/article/us-uganda-election/uganda-bans-social-media-ahead-of-presidential-election-idUSKBN29H0KH
76 https://www.business-humanrights.org/en/latest-news/uganda-shuts-down-internet-ahead-of-general-election/

kutoka nje katika uchaguzi ambapo kiongozi wa muda mrefu Yoweri Museveni alitangazwa mshindi dhidi ya Bobi Wine, mwimbaji maarufu aliyehamia siasa.[77]

1.8.

Muundo wa Muhtasari wa Sera

Wajibu wa watetezi wa haki za dijitali, waandishi wa habari, na wanaharakati wengine wa kijamii unathaminiwa zaidi wanapoonekana kusaidia kutatua changamoto mbalimbali zinazokabili jamii.

Hapa kuna zana za kazi[78] Kwa kuandaa muhtasari wa sera wenye ufanisi, na mifano ya muhtasari wa sera kama vile:

- Kutojihusisha kwa Afrika katika Teknolojia Mpya[79]
- Kutathmini ya mchakato wa mkataba wa Umoja wa Mataifa kuhusu masuala ya mtandao[80]
- Akili mnembe nchini Kenya[81]
- Udhibiti na Uchujaji wa Maudhui nchini Angola, Jamhuri ya Afrika ya Kati, na Jamhuri ya Kidemokrasia ya Kongo[82]
- Kuelekea Mpango wa Kitaifa wa Pamoja wa Biashara na Haki za Binadamu nchini Nigeria[83]

1.9.

Muundo wa Tamko la Pamoja

Kuongezeka kwa juhudi za serikali za Afrika kusimamia matumizi ya mitandao ya kijamii kupitia sheria zenye maneno yasiyo wazi au mapana kunapunguza uwazi wa mtandao, kuficha ukiukaji wa haki za binadamu, na kuunda vikwazo kwa utulivu wa muda mrefu na mazungumzo ya amani. Uwezo wa kupinga mwelekeo huu unaimarika wadau wanapoungana kwa sauti moja. Mifano ya kauli za pamoja zilizotolewa kushughulikia masuala haya ni pamoja na:

- Barua ya wazi ya mwaka 2023 iliyosainiwa na mashirika kadhaa kuhusu kufungiwa kwa Telegram nchini Kenya.[84]
- Tamko la pamoja la mwaka 2023 kwa niaba ya nchi 59 lililotolewa kwenye Baraza la Haki za Binadamu la Umoja wa Mataifa kuhusu hatari zinazozidi zinazohusiana na teknolojia za upelelezi na umuhimu wa hatua za kinga katika matumizi ya zana hizi.[85]
- Kikundi cha kimataifa cha mashirika na wataalamu kinaitaka serikali ya India iondoe Muswada wa Mawasiliano wa mwaka 2023

77 https://www.reuters.com/article/us-uganda-internet-rights-trfn-idUSKBN29P1V8/
78 https://socialwork.utoronto.ca/wp-content/uploads/2021/06/Policy-Toolkit-Final-v2-Apr27.pdf
79 https://paradigmhq.org/report/policy-brief-africas-absence-in-emerging-technologies/
80 https://paradigmhq.org/report/policy-brief-assesing-the-united-nations-cybertreaty-process/
81 https://paradigmhq.org/report/policy-brief-artificial-inteligence-in-kenya/
82 https://paradigmhq.org/report/policy-brief-censorship-and-content-moderation-in-angola-central-african-republic-and-democratic-republic-of-congo/
83 https://paradigmhq.org/report/policy-brief-towards-an-inclusive-national-action-plan-on-business-and-human-rights-in-nigeria/
84 https://www.accessnow.org/press-release/open-letter-clarification-on-telegram-blocking-in-kenya/
85 https://freedomonlinecoalition.com/joint-statement-heightened-risks-associated-with-surveillance-technologies-and-the-importance-of-safeguards-in-the-use-of-these-tools/

na kulinda haki za msingi.[86]

- Tamko la Muungano wa NetRights likilaani uvamizi wa teknolojia za kidijitali za wanaharakati wa asasi za kiraia nchini Zimbabwe wakati wa uchaguzi wa 2023.[87]
- Tamko la Muungano wa NetRights la mwaka 2023 likipinga udhibiti mpana wa mitandao ya kijamii nchini Nigeria.[88]

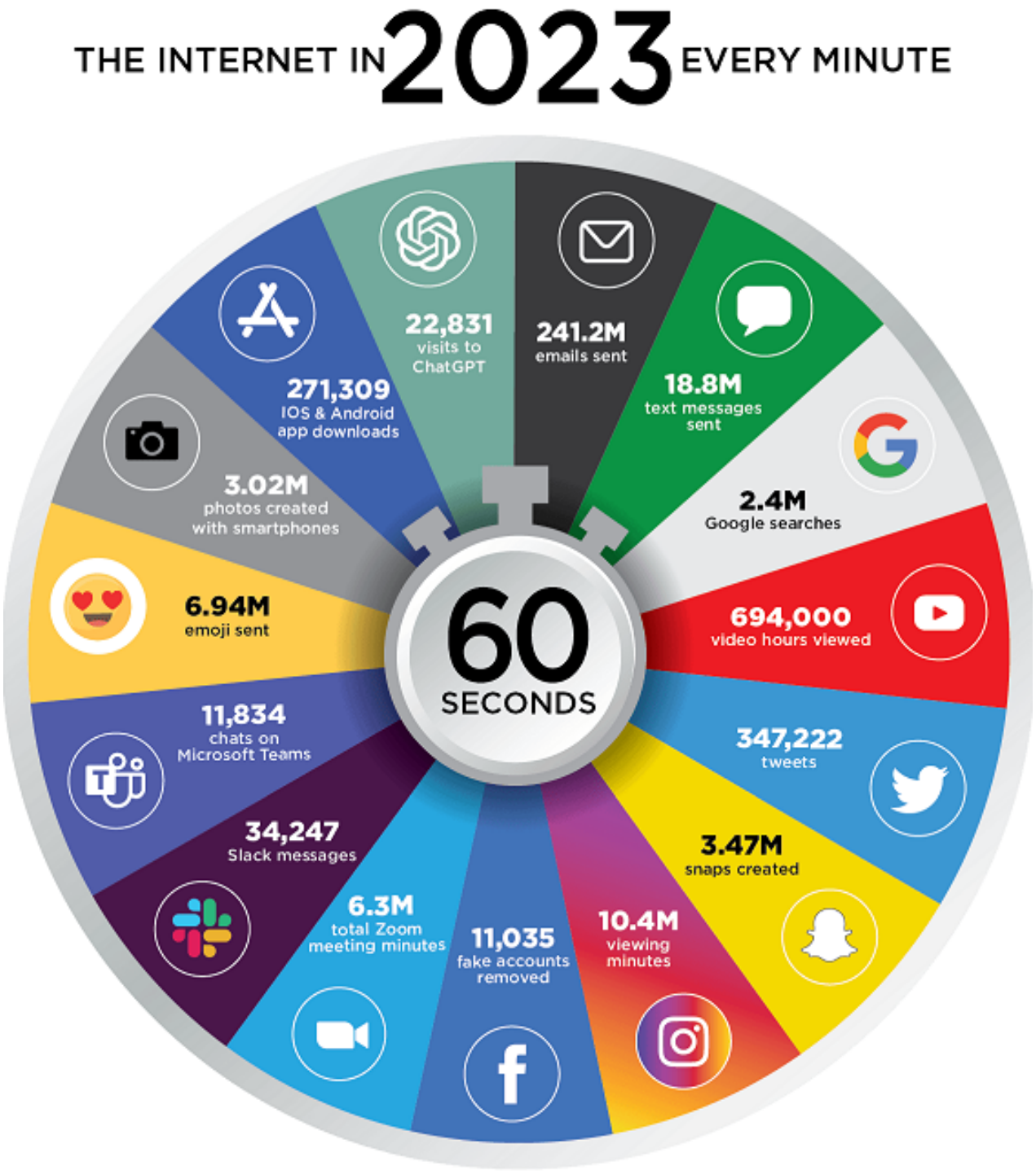
86 https://www.accessnow.org/press-release/india-must-withdraw-the-telecommunications-bill-2023/
87 https://paradigmhq.org/press-release-the-netrights-coalition-condemns-raids-of-digital-technologies-of-civil-society-actors-in-zimbabwe-during-the-2023-elections/
88 https://paradigmhq.org/the-netrights-coalition-strongly-condemns-the-call-for-blanket-social-media-regulation-in-nigeria/

SURA 02 | USALAMA NA UHAKIKA WA KIDIJITALI

Usalama wa kidijitali, pia hujulikana kama usalama wa mtandao, usalama mtandaoni, au usalama wa mtandao, unahusu mbinu na tahadhari mbalimbali zinazochukuliwa na mtu anapotumia mtandao ili kuhakikisha taarifa nyeti za kibinafsi na za vifaa vyake zinasalia salama.

Kulingana na «Infografiki ya Dakika Moja kwenye Mtandao» ya mwaka 2023,[89] Kila dakika, takriban barua pepe milioni 241.2, tweets 347,222, na ujumbe mfupi milioni 18.8 hutumwa kulingana na takwimu za ITU za mwaka 2023.[90]Hii inaonyesha kuwa zaidi ya watu bilioni 5.4, au asilimia 67 ya idadi ya watu duniani, wanatumia mtandao, na hivyo kuongeza idadi ya wahalifu mtandaoni, wadukuzi, vitisho, na udanganyifu mtandaoni kuliko hapo awali.

89 https://ediscoverytoday.com/2023/04/20/2023-internet-minute-infographic-by-ediscovery-today-and-ltmg-ediscovery-trends/
90 https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx


THE INTERNET IN 2023 EVERY MINUTE
22,831 visits to ChatGPT
241.2M emails sent
18.8M text messages sent
2.4M Google searches
694,000 video hours viewed
347,222 tweets
3.47M snaps created
10.4M viewing minutes
11,035 fake accounts removed
6.3M total Zoom meeting minutes
34,247 Slack messages
11,834 chats on Microsoft Teams
6.94M emoji sent
3.02M photos created with smartphones
271,309 IOS & Android app downloads
60 SECONDS
Created by: eDiscovery Today & LTMG

2.1.

Vitisho vya Usalama wa Kidijitali

Hapa ni baadhi ya vitisho vya usalama wa kidijitali ambavyo kila mtu anahitaji kufahamu.

Programu hasidi

Programu hasidi ni kifupi cha "programu hasidi." Ni programu au faili iliyoundwa kwa kusumbua, kuvamia, na kuleta hatari kwenye mfumo wa kompyuta na vifaa vya runununu. Mara nyingi huenezwa kupitia viambatisho vya barua pepe, ujumbe wa papo hapo (IM), kupakuliwa, udanganyifu na tovuti zinazopotosha. Mlipuko wa programu hasidi husababisha madhara kwa kuharibu data kwenye vifaa vilivyoathiriwa na/au kwa kusababisha msongamano wa mtandao ambao unaweza kuharibu kabisa mtandao. Aidha, programu hasidi inaweza kuwezesha washambuliaji kupata taarifa yoyote wanayotaka kutoka kwa kompyuta iliyoathiriwa, ikiwa ni pamoja na taarifa za kibinafsi za mwandishi wa habari, data, na vyanzo.

Aina za programu hasidi ni pamoja na:

Adware- ni aina ya programu ambayo inajisakinisha yenyewe kwa makusudi kwenye kifaa chako na imeundwa kutoa matangazo na madirisha ya pop-up ambayo hayakuhitajika.

Cryptojacking - Hii ni aina ya programu hasidi inayochukua udhibiti wa kifaa kwa lengo la kufanya uchimbaji wa Bitcoin, na hivyo kuongeza matumizi makubwa ya usindikaji kwenye kifaa ambacho kinaweza kupunguza kasi yake na kumaliza chaji ya betri haraka.

Ransomware - Hii ni aina ya programu hasidi iliyoundwa kuzuia ufikiaji wa mfumo wote au sehemu ya mfumo wa kompyuta hadi malipo yatolewe, ingawa malipo hayahakikishi kurudishiwa kwa ufikiaji. Kwa sababu wahalifu mara nyingi wanatarajia malipo ya haraka, walengwa mara nyingi ni taasisi kubwa (kama mashirika, idara za serikali, vyuo, na biashara) ambazo si tu zinaweza kuwa na rasilimali za kifedha, lakini pia zinapata hasara kubwa wakati huduma zao zinapozuiwa. Hata hivyo, watu binafsi bado wanaweza kuwa walengwa wa ransomware kwa sababu wanaweza kuwa mlango wa kuingilia mifumo ya taasisi hizo.

Spyware - Hii ni programu hasidi ambayo imesakinishwa kwa siri kwenye kompyuta au kifaa cha mkononi cha mtu ili kupata taarifa za kibinafsi za mmiliki, kama vile orodha za tovuti zilizotembelewa, maneno ya siri na nambari za kadi ya mkopo.[91]

Trojans - Hizi ni programu za ulaghai zinazopakuliwa kwa nia mbaya kwa kifaa ambacho huruhusu mhalifu wa mtandao ufikiaji wa mbali kwa

91 https://www.britannica.com/technology/spyware

kifaa mwenyeji, kuelekeza kifaa kwa aina mbalimbali za shughuli hasidi au uharibifu, au hata ufuatiliaji tu (kupeleleza) shughuli au mwingiliano kwenye kifaa.

Virusi / Viruses- Aina ya programu hasidi inayojiambatanisha na programu nyingine na ina uwezo wa kuenea kati ya vifaa na kusababisha uharibifu wa data na programu. Ikiwa virusi havitadhitiwa haraka, mtiririko wa barua pepe unaweza kusambaa kwenye seva, na kuharibu huduma za barua pepe kwa wote.

Minyoo/ Worms - ni aina ya programu hasidi ambayo hujirudia yenyewe kiotomatiki huenea kwenye kompyuta nyingine kwa njia ya mtandao.

Vidokezo vya Jinsi Programu Hasidi Inavyoweza Kuathri Kifaa Chako

- Uendeshaji wa mfumo wa polepole au kufungika mara kwa mara.
- Ongezeko la barua taka na matangazo yanayoibukia.
- Mifumo inayokataa kufanya kazi mara kwa mara.
- Alama zisizotambulika kwenye kifaa chako cha kazi.
- Kuhamishwa sehemu ya awali ya tovuti kutoka kwa tovuti maarufu hadi zisizo julikana.
- Kuundwa kwa faili au folda mpya bila idhini yako.
- Upungufu wa haraka wa chaji ya betri.

Vitisho vya Ufuatiliaji wa Kidijitali

Inajumuisha kufuatilia mahali, kutambua uso, kufuatilia watu wengi, na kuingilia mawasiliano. Ufuatiliaji una athari mbaya kwa uwezo wa waandishi na watafiti kuendelea na kuchapisha hadithi, na kuwafanya iwe ngumu kulinda vyanzo vyao.

Mashambulizi ya Uhandisi wa Kijamii

Uhandisi wa kijamii ni mbinu inayotumiwa kuwahadaa watumiaji kufichua taarifa fulani, kutekeleza kitendo mahususi kwa sababu zisizo halali, au kutoa mahali pa kuingilia kwa programu hasidi. Hili linaweza kuwa jaribio la mtu usiyemjua kupata maelezo kutoka kwako ambayo kwa kawaida hungeshiriki mtandaoni, kwa mfano maelezo ya kadi ya mkopo, tarehe ya kuzaliwa, mahali unapopenda likizo, jina la mnyama kipenzi. Je, wanahitaji taarifa hizo kweli? Majibu ya maswali haya yanaweza kusababisha akaunti kuathiriwa.

Baadhi ya aina za uhandisi wa kijamii ni pamoja na:

Mashambulizi ya hadaa (Phishing attacks) - Kampeni za «Hadaa» au «hadaa kwa kutumia mkuki» mara nyingi hutumia viungo au viambatisho kwenye barua pepe au mitandao ya kijamii

ambazo hubeba programu hasidi. Mara viungo hivi vinapo bofya, vinaweza kusababisha uharibifu mkubwa.[92]

Shambulio la Ujumbe Hadaa (Smishing) - Pia inajulikana kama SMS-hadaa, ni aina ya shambulio la uhandisi wa kijamii linalofanywa kupitia ujumbe mfupi. Katika shambulio hili, walaghai hujaribu kumshawishi mtumiaji kubofya kiungo kinachompeleka kwenye tovuti hasidi..[93]

Udanganyifu rununu (Vishing) - Njia ya uhandisi wa kijamii ambapo watu hudanganywa ili kutoa taarifa nyeti kupitia simu au ujumbe wa sauti.[94]

Mtego (Baiting) - Aina ya shambulio la uhandisi wa kijamii ambapo walaghai hutoa kitu cha thamani kwa mwathiriwa ili kupata taarifa nyeti za kibinafsi kutoka kwake. Kwa mfano, mwathiriwa anaweza kupokea barua pepe inayomwahidi kadi ya zawadi bila malipo kwa kubofya kiungo.[95]

Kujinadi (Pretexting) - Aina ya uhandisi wa kijamii ambapo wahalifu wa mtandao hujifanya kuwa chanzo cha kuaminika ili kuwashawishi waathiriwa kutoa taarifa muhimu au nyeti.[96]

Mashambulizi ya Tovuti Bandia

Hizi ni tovuti zinazoundwa kwa lengo la kuiga tovuti halali kwa madhumuni mabaya. Vyombo vya habari huru na tovuti za mashirika ya kiraia mara nyingi huwa waathirika. Tovuti hizi bandia hutumika kusambaza programu hasidi au kuchapisha habari za uwongo ili kudharau tovuti halisi ya vyombo vya habari au mwandishi fulani.

Mashambulizi ya mtu wa kati (MitM).

Shambulio la mtu wa kati ni shambulio la mtandao ambapo mshambuliaji hunasa kwa siri mawasiliano kati ya watu wawili au zaidi wanaoamini kuwa wanawasiliana moja kwa moja.[97] Kwa mfano, kipanga njia cha Wi-Fi kinasanidiwa kama mtandao bandia wa Wi-Fi katika eneo la umma ili kuwahadaa watu kufikiri kuwa ni halali. Watu wanapojiunga na mtandao huo, mshambuliaji anapata moja kwa moja data zote zinazopita kupitia kipanga njia hicho.

Mashambulizi ya Kutopatikana kwa Huduma ya mtandao kwa Kusambaratishwa (DDoS).

Mashambulizi haya ni ya kawaida sana na yanahusisha kompyuta moja au zaidi na miunganisho ya mtandao inayolenga seva na kuisumbua, kuzuia watu wengine kuiweza. Kwa tovuti za habari, mashambulizi haya

92 https://www.exabeam.com/information-security/cyber-security-threat/
93 https://www.aura.com/learn/types-of-social-engineering-attacks
94 https://www.exabeam.com/information-security/cyber-security-threat/
95 https://www.aura.com/learn/types-of-social-engineering-attacks
96 https://www.aura.com/learn/types-of-social-engineering-attackshttps://www.aura.com/learn/types-of-social-engineering-attacks
97 https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/man-in-the-middle-attack-mitm/

husababisha kizuizi cha upatikanaji wa habari kwa umma na mara nyingi huleta gharama kubwa kutokana na kupungua kwa idadi ya wageni na haja ya msaada wa kiufundi.

Ufuatiliaji wa Mtandao

Matumizi ya mtandao au njia za elektroniki kufuatilia na/au kudhuru mtu binafsi, kundi, au shirika. Inaweza kujumuisha kutoa mashtaka ya uwongo, kashfa, au matusi. Pia inaweza kuhusisha ufuatiliaji, wizi wa utambulisho, vitisho, uharibifu, au kukusanya taarifa ambazo zinaweza kutumiwa kwa lengo la kutishia, kuaibisha, au kudhuru.

Unyanyasaji wa Mtandaoni

Matumizi ya njia za elektroniki kama vile barua pepe, mitandao ya kijamii, ujumbe wa papo kwa papo, na njia zingine za mawasiliano mtandaoni kwa lengo la kutumia vibaya, kutishia, au kumshinda mtu binafsi au kikundi.

Hatua za Kuzuia Tishio la Kidijitali

Jitihada kidogo zinaweza kusaidia kulinda kompyuta yako na kuzuia matatizo mengi zaidi. Hatua zifuatazo zitakusaidia kuzuia mashambulizi au kukabiliana na virusi ikiwa kompyuta itaambukizwa:[98]

- **Sakinisha programu ya kuzuia virusi:** Zana za kuzuia programu hasidi husaidia kugundua na kuondoa programu zisizo salama kutoka kwa kompyuta au kifaa chako cha rununu**.**
- **Sasisha programu:** Hakikisha kuwa unasasisha programu zote. Programu ambazo hazijasasishwa na zisizo na alama za usalama za hivi karibuni zinaweza kuwa hatarini kwa programu hasidi.
- **Weka mipaka ya ufikiaji wa faili zako za mtandao:** Ruhusu tu kiwango cha ufikiaji kinachohitajika kwa utendaji wa biashara ya mtumiaji. Kupunguza ushiriki wa faili za mtandao kutazuia kifaa kilichoathiriwa na ransomware kuisambaza kwa vifaa vingine kwenye mtandao.
- **Epuka kufungua au kutekeleza viambatisho visivyotarajiwa.**
- Zima kipengele cha ukaguzi katika programu zako ili kuongeza usalama.
- Zima sehemu yoyote ya programu ambayo inaweza kufungua barua pepe, ujumbe wa papo kwa papo, kiambatisho cha faili au kupakua kiotomatiki.

2.2.

Usafi wa Kidigitali

Kwa lengo la kuhakikisha usalama wa kidijitali kwa wanahabari, watetezi wa haki za kidijitali, na watumiaji wengine wa mtandao, kuna seti ya hatua za usafi wa kidijitali zinazopatikana kusaidia kuzuia vitisho na matukio ya usalama wa kidijitali.

98 https://it.osu.edu/security

Usafi wa kidijitali (au usafi wa mtandao) ni mazoea na tabia zinazohusiana na kusafisha na kudumisha ulimwengu wetu wa kidijitali. Hii ni pamoja na shughuli kama kupanga faili kwenye vifaa vyako vya kidijitali, kulinda utambulisho wako mtandaoni na data yako, na kusakinisha programu au teknolojia mpya ili kuongeza usalama na urahisi wa maisha yako ya kidijitali.

Njia mojawapo ya kupunguza hatari ya kushambuliwa mtandaoni na kukabiliana na athari za mashambulizi ni kuhakikisha ulinzi wa maelezo unayoshiriki na vifaa unavyotumia. Kila kitu unachochapisha mtandaoni kinaweza kutumiwa na watu wasiokuwa na nia njema kuanzisha udanganyifu au mashambulizi dhidi yako. Kama mtetezi wa haki za kidijitali, ni muhimu kufuata kanuni bora za usafi wa kidijitali ili kuhakikisha usalama wako mtandaoni..

Sehemu iliyobaki inaelezea shughuli rahisi unazoweza kufanya bila kutumia teknolojia ghali au kutumia muda mrefu kuweka upya mtandao wako wa nyumbani, ili kuboresha usalama wa kompyuta yako mtandaoni.

2.3.

Nywila

Ikiwa unatafuta njia ya kuimarisha usalama wa mtandao wako, anza na usalama wa neno la siri. Nenosiri ni muhimu katika kulinda ufikiaji wako, kwa kutumia herufi za alfabeti, nambari, na ishara au mchanganyiko wa hizo. Hii njia ya usalama huzuia ufikiaji usiohalali wa mfumo, programu, au huduma kwa watumiaji wasio na idhini.

Mazoezi ya kawaida ya usalama wa digitali ni pamoja na kuunda neno la siri imara, kutoitumia tena, kutumia uthibitishaji wa hatua mbili, kushughulikia kwa uangalifu maswali ya kurejesha nenosiri, kutoandika neno la siri, na mwishowe, kutumia usimbuaji wa nenosiri.

Zana za kuzalisha neno la siri

Zana za kuzalisha neno la siri ni programu inayosaidia kuunda neno la siri la nasibu au lenye sifa maalum kwa watumiaji. Inawezesha watumiaji kutengeneza nenosiri imara zaidi ambalo linaboresha usalama kwa aina fulani ya ufikiaji.

Zana za kuzalisha neno la siri zinasaidia watu ambao wanahitaji kuunda nywila mpya mara kwa mara ili kuhakikisha ufikiaji ulioidhinishwa kwa programu na kusimamia idadi kubwa ya nywila kwa utambulisho na usimamizi wa ufikiaji.

Wasimamizi wa nywila

Kidhibiti cha nywila ni zana ambayo hujenga na kuhifadhi wa nywila kadhaa , kuruhusu matumizi ya manenosiri mbalimbali kwa tovuti na huduma tofauti bila hitaji la kuyakumbuka.

Wasimamizi wa nywila

- Weka nywila lenye usalama ambalo hakuna mtu mwenye uwezo wa kudhania.
- Hifadhi nywila kadhaa (na majibu kwa maswali ya usalama) kwa usalama
- Hifadhi nywila zote kwa kutumia

nenosiri kuu (au neno la siri) moja.[99]

Ikiwa kompyuta au kifaa chako kitashambuliwa na programu ya kupeleleza ikasakinishwa, inaweza kukusanya habari unapoingiza nywila yako kuu na hata kuiba data zako za kidhibiti cha nywila. Hivyo, ni muhimu sana kuhakikisha kuwa kompyuta yako na vifaa vingine vimesafishwa na salama dhidi ya programu hasidi unapotumia kidhibiti cha nywila.

Kumbuka!

Kutumia vidhibiti vya nywila *ni kama kuweka mayai yako yote kwenye kapu moja na kuyalinda maishani mwako. Hatari ya wasimamizi wa* nywila *waliodukuliwa ni kwamba ufikiaji wa "kikapu" unamaanisha ufikiaji wa "mayai" yako yote.*

Kusawazisha nywila kwenye vifaa vingi[100]

Wasimamizi wengi wa nywila huruhusu upatikanaji wa nywila kwenye vifaa vyote kupitia kipengele cha kusawazisha nywila. Hii inamaanisha kwamba unaposawazisha faili ya nywila kwenye kifaa kimoja, inapatikana moja kwa moja kwenye vifaa vingine vyote. Vidhibiti vya nywila vinaweza kuhifadhi nywila "kwenye wingu," ikimaanisha kwamba zimesimbwa kwa usalama kwenye seva ya mbali. Wakati nywila zinahitajika, wasimamizi hawa watapata na kuzisimbua.[101] Kutumia vidhibiti vya nywila ambavyo hutumia seva zao wenyewe kwa kuhifadhi au kusaidia kusawazisha nywila ni rahisi, lakini inaweza kuwa hatari zaidi ya kushambuliwa. Ikiwa nywila zimehifadhiwa kwenye kompyuta na wingu, mshambuliaji hahitaji kuiba kompyuta ili kuzipata nywila (lakini badala yake wanahitaji kuvunja usimbaji wa nywila wa vidhibiti vya nywila). Ikiwa hili linawezekana, ni vyema kuepuka kusawazisha nywila kwenye wingu na badala yake kuzihifadhi kwenye vifaa vyako pekee.

Kumbuka!

Ni muhimu kuweka nakala rudufu ya hifadhidata ya nywila tu kama tahadhari. Kuhifadhi nakala rudufu ni muhimu katika kesi hifadhidata ya nywila inapopotea kutokana na athari za mfumo au upoteaji wa kifaa. Vidhibiti vya nywila mara nyingi hutoa njia ya kujenga faili za nakala rudufu, au mtu anaweza kutumia programu ya kawaida ya kuhifadhi nakala.

Mashambulizi ya kawaida ya nywila

Mbinu moja rahisi na ya kawaida ya kuingia kwenye akaunti ni kujaribu[102] Nywila za kawaida au kufanya utafiti mdogo kuhusu mtu anayelengwa na kujaribu nywila fulani zinazohusiana naye. Ripoti ya Cybernews ya 2024 ilifunua kuwa nywila 10 za juu

99 https://ssd.eff.org/glossary/passphrase
100 https://ssd.eff.org/en/module/creating-strong-passwords#3
101 https://ssd.eff.org/glossary/decrypt
102 https://edition.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html

zilizotumiwa sana na zilizodukuliwa zilikuwa:

1. 123456
2. 123456789
3. qwerty
4. Nywila
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

Hizi ni nywila ambazo si salama KABISA. Ni rahisi kubashiri na wahalifu wa mtandao mara nyingi huanza kujaribu kufikia akaunti kwa kutumia nywila dhaifu kama hizi.

KAMWE usitumie nywila ambazo zina sifa zifuatazo:

- Jina lako au majina ya familia yako na marafiki,
- Siku yako ya kuzaliwa au ya familia yako na marafiki,
- Majina ya wanyama na
- Majina ya sehemu ulizoishi au ulikokuwa, ikiwa ni pamoja na majina ya miji au mitaa.

Inastaajabisha ni jinsi gani taarifa nyingi kuhusu mtu zinapatikana kwenye mtandao. Hivyo, ikiwa nenosiri lako linajumuisha taarifa zinazoweza kutambuliwa kwa urahisi kutoka kwenye mtandao au kwa mazungumzo na marafiki zako, linaweza kutabiriwa kwa urahisi.

Shambulizi la Nguvu

Shambulio la nguvu linalojaribu kila mchanganyiko wa wahusika unaowezekana hadi linapata nywila sahihi. Aina hii ya shambulio ni nzuri kwa nywila fupi na inaweza hata kuvunja nywila zenye herufi zilizo changanywa kwa nasibu. Hata hivyo, urefu wa nywila siyo jambo la kipaumbele. Mashambulio ya nguvu hayana ufanisi sana, na ikiwa nenosiri lako ni refu vya kutosha, linaweza kuwa gumu kudukuliwa. Angalia jedwali ambalo linaonyesha muda utakaohitajika kugundua nenosiri katika mashambulio ya nguvu, ukizingatia urefu na utata wa nywila. Ni muhimu kuzingatia kwamba jedwali hili linahusu uwezo wa kompyuta kujaribu zaidi ya nywila 1000 kwa sekunde.

Urefu wa Nywila	Herufi zote	Herufi ndogo tu
3 herufi	0.86 sekunde	0.02 sekunde
4 herufi	1.36 dakika	0.46 sekunde
5 herufi	2.15 masaa	11.9 sekunde
6 herufi	8.51 siku	5.15 dakika
7 herufi	2.21 miaka	2.23 masaa
8 herufi	2.10 karne	2.42 siku
9 herufi	20 milenia	2.07 miezi
10 herufi	1,899 milenia	4.48 miaka
11 herufi	180,365 milenia	1.16 karne
12 herufi	17,184,705 milenia	3.03 milenia
13 herufi	1,627,797,068 milenia	78.7 milenia
14 herufi	154,640,721,434 milenia	2,046 milenia

Kumbuka kuwa muda wa kudukua nywila huongezeka kwa kasi kila wakati unapoongeza herufi. Kwa mfano, kwa nywila lenye wahusika wa aina zote wa kubahatisha, tofauti kati ya nywila lenye urefu wa wahusika 6, 7, 8 na 9 ni kuhusu siku, miaka, karne na milenia! Pia, angalia ni muda gani unahitajika kudukua nywila lenye aina zote za herufi ikilinganishwa na nywila lenye urefu sawa ambalo linatumia herufi ndogo tu.

Kuunda na Kudumisha Nywila Imara na Salama

Kutumia nywila ile ile mara kwa mara ni hatari kwa usalama. Mtu mbaya akipata nywila lako linalotumiwa kwa huduma nyingi, wanaweza kupata ufikiaji wa akaunti zako zote. Hii ni sababu kuu ya kuwa na nywila nyingi, imara, na za kipekee. Kwa bahati nzuri, wasimamizi wa nywila wanaweza kusaidia katika hili.[103]

Vidokezo vya kuunda nywila imara

- Tumia mchanganyiko wa herufi kubwa na ndogo, nambari na alama za ishara.
- Nywila imara linapaswa kuwa kati ya wahusika nane na kumi na mbili.
- Epuka kutumia data ya kibinafsi.
- Geuza mara kwa mara.
- Kamwe usitumie kwenye akaunti zaidi ya moja.
- Tumia uthibitishaji wa hatua mbili.

Kuna nywila chache ambazo unahitaji kukumbuka na zinapaswa kuwa imara sana. Hizi ni pamoja na:

- nywila za kifaa chako
- nywila za usimbaji (kama usimbaji wa diski nzima)[104]
- Nywila kuu,[105] au “kaulisiri”[106] kwa msimamizi wako wa nywila
- Nywila yako ya barua pepe[107]

Kutengeneza nywila imara kwa kutumia kete

Moja ya matatizo makubwa wakati watu wanapochagua nywila wenyewe ni kwamba hawana uwezo mzuri wa kufanya chaguo ambazo ni nasibu na zisizotabirika.[108] Njia bora ya kuunda nywila imara na rahisi kukumbuka [109] ni kutumia kete[110] na orodha ya maneno [111] kuchagua maneno kwa nasibu. Maneno haya yakijumuishwa yanaunda “kaulisiri” yako. “Kaulisiri” ni aina ya nywila ambayo ni ndefu ili kutoa usalama wa juu zaidi. Kwa usimbaji wa diski na msimamizi wako wa nywila, tunapendekeza kutumia angalau maneno sita.

Kwa nini utumie angalau maneno sita? Kwa nini utumie kete kuchagua maneno kwa nasibu katika kaulisiri?

Kwa kuwa na nywila ndefu na isiyo na mpangilio, inakuwa vigumu zaidi kwa kompyuta na wanadamu kubashiri. Ili kuelewa kwa nini unahitaji nywila ndefu na ngumu, angalia maelezo ya video haya.[112]

103 https://ssd.eff.org/en/glossary/password-manager
104 https://ssd.eff.org/en/glossary/encryption
105 https://ssd.eff.org/glossary/master-password
106 https://ssd.eff.org/en/glossary/passphrase
107 https://ssd.eff.org/en/glossary/password
108 http://people.ischool.berkeley.edu/~nick/aaronson-oracle/
109 https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases
110 https://www.eff.org/dice
111 https://www.eff.org/deeplinks/2018/08/dragon-con-diceware
112 https://ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using-dice

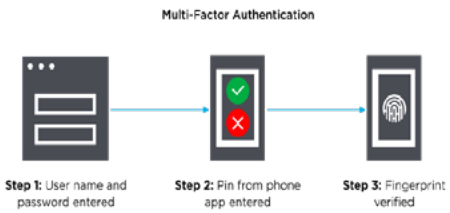
2.4.

Uthibitishaji wa hatua nyingi (MFA)

Nywila imara na za kipekee hufanya iwe ngumu sana kwa wahalifu kupata ufikiaji wa akaunti zako za kidijitali. Ili kuongeza ulinzi kwa akaunti zako, wezesha uthibitishaji wa hatua mbili.[113]

Uthibitishaji wa hatua nyingi ni sehemu ya usalama inayopatikana kwenye tovuti nyingi, programu, na vifaa ambavyo vinaboresha usalama wa akaunti kwa kutoa njia mbili au zaidi za uthibitisho.

Jinsi uthibitisho wa hatua mbili unavyofanya kazi



Ukiwa umewezesha uthibitishaji wa hatua mbili kwa akaunti yako (kwenye wavuti, programu, au kifaa), unapoingia kwa kutumia jina lako la mtumiaji na nywila, seva ya akaunti itahitaji uthibitisho wa ziada kabla ya kuruhusu ufikiaji. Hii inalingana na mchakato wa benki ambapo wanaweza kuuliza vitambulisho vya picha na vifaa vingine kama Kadi ya Usalama wa Jamii au pasipoti. Uthibitisho wa hatua mbili unafanya iwe ngumu kwa mtu yeyote kujifanya kuwa wewe ni wewe wakati wanahitaji uthibitisho kutoka kwa vyanzo tofauti viwili.

Njia za uthibitishaji wa hatua mbili

Tunapendekeza kujiandikisha angalau vifaa viwili kwa uthibitishaji wa hatua mbili. Hii itakusaidia kulinda akaunti yako ikiwa kifaa kimoja kitapotea; unaweza kufuta data yake kwa mbali na kutumia kifaa kingine kuthibitisha upatikanaji. Na Uthibitishaji wa hatua nyingi (MFA), unaweza kutumia njia mbalimbali kwa ajili ya uthibitisho wa pili.

Njia za mara kwa mara ni pamoja na:

Maombi ya simu za mkononi ya «kusukuma taarifa»

Njia maarufu ya kupata fomu ya pili ya uthibitishaji ni kupitia “kusukuma taarifa” kwa programu kwenye simu yako ya mkononi. Kwa njia hii, seva ya akaunti unayojaribu kuingia itatuma arifa kwenye simu yako ya mkononi. Arifa itaonekana kwenye simu yako na itakuwa na ujumbe kama, “Kuna jaribio la kuingia kwenye tovuti hii, je, ni wewe?” Mara nyingi kuna kitufe cha kijani kibichi na cha kijani kikubwa ambacho unaweza kubonyeza “ndio” au “hapana” kwa urahisi. Kama ukibonyeza “ndio”, utapata ufikiaji. Lakini kama haukutegemea ombi la kuingia, inaonyesha mtu mwenye neno lako la siri anajaribu kuingia kwenye akaunti yako. Unaweza kubonyeza “hapana” na ufikiaji wao utakataliwa. Kisha unaweza kuchukua

113 https://ssd.eff.org/en/glossary/two-factor-authentication

hatua ya kujilinda na kubadilisha neno lako la siri ili mshambulizi asiweze kuingia tena.

Ni rahisi kutumia, lakini ni hatua muhimu ya usalama. Faida kuu ya njia hii ni kwamba mshambuliaji anahitaji si tu kubadilisha nywila yako, lakini pia lazima apate ufikiaji wa simu yako ya mkononi na aweze kuingia kwenye kifaa hicho. Hatari ya hili kutokea yote ni ndogo sana ikiwa unatumia nywila imara na unalinda simu yako vizuri. Faida nyingine ya njia hii ni kwamba unapokea arifa mara moja mtu anapojaribu kuingia kwenye akaunti yako, hivyo unaweza kuchukua hatua haraka kwa kubadilisha nywila yako.

Programu za uthibitishaji wa kifaa cha simu

Wakati mwingine, badala ya kutuma arifa ya kushinikiza, seva ya akaunti inaweza kukuhitaji uchapishe nambari ya kipekee iliyotolewa na programu ya Uthibitishaji kwenye simu yako ya mkononi. Nambari hizi ni fupi (kawaida takriban nambari 6 au zaidi), na inaweza kuonekana si salama sana kwa sababu ya urefu wake. Hata hivyo, nambari hizi zinatengenezwa upya kila dakika na zinategemea nambari ambayo ni ya kipekee kwa programu yako ya Uthibitishaji na seva ya akaunti unayojaribu kuunganisha nayo. Hii inafanya iwe ngumu sana kwa wahalifu wa mtandao kudhani nambari sahihi za 6 chini ya hali hizo kwa sababu muda wa nambari hizo ni mfupi sana.Faida kuu hapa ni kwamba mshambuliaji lazima awe na ufikiaji wa kimwili kwa simu yako ya mkononi na uwezo wa kuingia ndani yake ili kupata nambari hizo. Kando na hayo, unakosa arifa ya wakati halisi ikiwa kuna jaribio la kuingia kwenye akaunti yako. Kawaida, njia hii hutumiwa kama mbadala ya kushinikiza pia. Programu nyingi za uhakiki zinaweza kusaidia na njia zote mbili hizi.

Njia ya kuweka msimbo wa SMS

Hii njia pia hutumia simu yako ya mkononi lakini haitegemei programu. Kwa hiyo, inafanya kazi na simu ambazo niyo rununu. Wakati unapochagua kutumia njia hii ya Uthibitishaji wa hatua nyingi (MFA), baada ya kuingia na jina lako la mtumiaji na nywila, seva ya akaunti itatuma ujumbe wa maandishi na nambari ya wakati mmoja kwenye simu yako ya mkononi. Halafu utaiweka nambari hiyo kwenye wavuti au kifaa ulichotumia kuingiza nenosiri lako. Hii ina faida sawa na njia ya “kushinikiza”, isipokuwa unahitaji kuweka nambari hiyo kwa mkono. Utapokea arifa halisi wakati kuna jaribio la kuingia na utapata ujumbe wa maandishi kuhusu jaribio hilo. Kwa upande mwingine, shambulizi haliwezi kufanikiwa bila mshambuliaji kuwa na simu yako, kwani ujumbe wa maandishi mara nyingi huonekana kwenye skrini ya simu, hata kama simu imefungwa.

Njia ya mifumo ya barua pepe

Njia hii inafanya kazi kama njia ya SMS, lakini badala ya kutuma nambari kupitia SMS, inatumwa kwa anwani ya barua pepe ya akaunti ambayo umesajiliwa kwenye seva ya akaunti unayotaka kupata. Kawaida unaweza kuweka hii wakati unajiandikisha kwa huduma ambazo unatumia mara kwa mara. Ikiwa utatumia aina hii ya Uthibitishaji wa hatua nyingi (MFA), lazima uhakikishe kuwa akaunti yako ya barua pepe imehifadhiwa vizuri, na hii inaweza kumaanisha kwamba unapaswa kuwezesha Uthibitishaji wa hatua nyingi (MFA) kwa ufikiaji wa akaunti yako ya barua pepe. Hii ni kwa sababu barua

pepe inaweza kufikiwa kutoka mahali popote, pamoja na kompyuta ile ile ambayo mhalifu wa mtandao anajaribu kuingia kwenye akaunti yako. Kwa maneno mengine, njia hii haimaanishi kwamba unapaswa kuwa na kifaa maalum ambacho kinahitaji ufikiaji wa kimwili. Hivyo ndivyo unavyopaswa kuwa na nywila imara kwa barua pepe yako ambayo haitumiki mahali pengine popote. Kwa kufanya hivyo, mshambuliaji kimsingi atahitaji kujua nywila zako zote mbili ili kupata mafanikio. Hata hivyo, kuwalazimisha kutumia kifaa kingine ni chaguo lenye nguvu na salama zaidi. Ikiwa tovuti inahitaji Uthibitishaji wa hatua nyingi (MFA) ya aina hii tu, hiyo ni sahihi. Endelea na usanidi, kisha omba uthibitisho kwa kutumia simu yako ya mkononi kwa ufikiaji wa barua pepe yako.

Tokeni Halisi

Njia hii ilijulikana sana kabla ya ujio wa simu mahiri. Tokeni halisi ni kifaa kidogo kinachotengeneza misimbo mfululizo sawa na programu ya uthibitishaji kwenye simu yako ya mkononi. Inafanya kazi sawa, lakini ina changamoto ya ziada ya kuhitaji kufuatilia kifaa hiki cha ziada. Siku hizi, maisha yetu yameunganishwa na simu zetu za rununu. Unaweza kufikiria hatari ya kupoteza tokeni na kutogundua kuwa imepotea kwa muda. Ikiwa una moja ya hizi, iweke mahali salama. Ikiwa unahitaji kuibeba nawe, jaribu kuifunga kwenye funguo zako.

Biometriki

MFA ya kibayometriki hutumia sifa za kipekee za kimwili au kitabia za mtumiaji, kama vile utambuzi wa uso, uchanganuzi wa alama za vidole, uchanganuzi wa mboni ya jicho, na utambuzi wa sauti. Kwa kuwa kila mtu ana alama za vidole na uso wa kipekee, hii inaweza kuwa njia salama sana. Biometriki hutumiwa mara nyingi kama Uthibitishaji wa hatua nyingi (MFA) kwa programu zilizo na data nyeti.

Uthibitishaji wa hatua nyingi (MFA) ya kibayometriki inaweza kutoa kiwango cha juu zaidi cha uhakikisho kwamba mtumiaji ndiye anayedaiwa kuwa, kwani data ya kibayometriki ni ngumu kughushi, kuiba, au kukisia ikilinganishwa na nywila au tokeni. Hata hivyo, ina changamoto zake, kama vile masuala ya faragha. Mifumo ya uthibitishaji wa kibayometriki huhifadhi taarifa nyeti, na ikiwa taarifa hii itaangukia mikononi mwa watu wasiofaa, inaweza kutumika kwa wizi wa utambulisho au madhumuni mengine mabaya. Pamoja na changamoto hizi, uthibitishaji wa kibayometriki ni wa kutegemewa na ni mgumu zaidi kuvunja ikilinganishwa na mbinu nyingine za uthibitishaji. Kuna njia za kupunguza hatari za usalama kwa kutumia kwa uangalifu mazoea ya ziada ya usalama, kama vile kuchanganya biometriki na mambo mengine ya uthibitishaji kupitia Uthibitishaji wa hatua nyingi (MFA) ili kutoa safu ya ziada ya ulinzi.

2.5.

Uthibitishaji wa Vipengele Viwili (2FA).

Uthibitishaji wa Vipengele Viwili (2FA) ni aina ya Uthibitishaji wa hatua nyingi (MFA) ambapo watumiaji wanajitambulisha kwa watoa huduma kwa kutumia mchanganyiko wa mbinu mbili tofauti za uthibitishaji. Hizi mbinu zinaweza kuwa kitu ambacho mtumiaji anajua (kama nywila au PIN), kitu ambacho mtumiaji anacho

(kama tokeni ya maunzi au simu ya mkononi), au kitu ambacho ni sehemu ya mtumiaji (kama alama za vidole).

Je, 2FA inafanya kazi vipi kwenye mtandao?

Huduma kadhaa za mtandaoni - kama vile Facebook, Google, na X - zinatoa 2FA kama mbadala wa uthibitishaji wa nywila pekee. Ukiwasha kipengele hiki, utaombwa kuingiza nenosiri pamoja na mbinu ya pili ya uthibitishaji. Njia hii ya pili mara nyingi huwa ni msimbo wa mara moja unaotumwa kupitia SMS au msimbo wa mara moja unaozalishwa na programu maalum ya simu inayohifadhi siri, kama vile Google Authenticator au Duo Mobile.IKwa vyovyote vile, kipengele cha pili ni simu yako ya mkononi, kitu ambacho (kawaida) unamiliki. Baadhi ya tovuti (ikiwa ni pamoja na Google) pia zinaunga mkono misimbo mbadala ya matumizi moja, ambayo inaweza kupakuliwa, kuchapishwa, na kuhifadhiwa mahali salama kama hifadhi rudufu. Baada ya kuchagua kuingia kwa kutumia 2FA, utahitaji kuingiza nywila lako pamoja na msimbo wa mara moja kutoka kwenye simu yako ili kufikia akaunti yako.

Kwa nini unapaswa kuwasha 2FA?

2FA inakupa usalama zaidi wa akaunti kwa kukuhitaji kuthibitisha utambulisho wako kwa kutumia mbinu zaidi ya moja. Hii inamaanisha kwamba, hata kama mtu angefanikiwa kupata nenosiri lako, hawezi kufikia akaunti yako bila kuwa na simu yako ya mkononi au njia nyingine ya pili ya uthibitishaji.

Je, kuna changamoto au upungufu wowote wa kutumia 2FA?

Licha ya kutoa njia salama zaidi ya uthibitishaji, 2FA ina hatari kubwa ya kufungiwa nje ya akaunti yako ikiwa, kwa mfano, utapoteza au kubadilisha vibaya SIM kadi yako.[114] Au kusafiri hadi nchi bila kuingia kwenye uzururaji. Aidha, kutumia 2FA kunamaanisha kuwa unaweza kutoa maelezo zaidi kwa huduma kuliko ilivyostahiliwa. Kwa mfano, sema unatumia huduma X na umejiandikisha kwa kutumia jina la uongo.[115] Hata kama unajitahidi kuepuka kutoa maelezo yako ya kibinafsi kwa X, na unatumia huduma kupitia Tor au VPN pekee .[116] Kwa kuwezesha SMS 2FA, X atahitaji kuwa na rekodi ya nambari yako ya simu. Hii ina maana kwamba, ikihitajika na mahakama, X inaweza kuunganisha akaunti yako na wewe kupitia nambari yako ya simu. Hii inaweza isiwe tatizo ikiwa tayari unatumia jina lako halali kwenye huduma hiyo, lakini ikiwa kubaki bila kutambuliwa ni muhimu kwako, chunguza kwa makini kabla ya kuamua kutumia SMS 2FA.

Uthibitishaji wa Kipengele cha wote

Uthibitishaji wa wote, unaojulikana pia

114 https://ssd.eff.org/en/glossary/sim-card
115 https://ssd.eff.org/en/glossary/pseudonym
116 https://ssd.eff.org/en/glossary/vpn

kama kuingia mara moja (SSO), ni mbinu ya uthibitishaji wa utambulisho wa mtandao inayowaruhusu watumiaji kuhamia kutoka tovuti moja hadi nyingine kwa usalama bila kuhitaji kuingiza taarifa ya kutambua mara kwa mara. Kwa kutumia uthibitishaji wa wote, mteja huingiza seti moja ya vigezo (kama vile jina la mtumiaji na nenosiri) mwanzoni mwa kila kipindi cha mtandao. Taarifa ya uthibitishaji kwa tovuti yoyote inayotembelewa baadaye hutolewa kiotomatiki kwa muda wa kipindi hicho. Moja ya changamoto kubwa za usalama wa mtandao ni kwamba kila tovuti ina mfumo wake wa uthibitishaji. Mtumiaji wa kawaida wa mtandao, ambaye ana anwani mbili au tatu za barua pepe za wavuti na anatembelea wachuuzi kadhaa mtandaoni kununua au kuuza vitu, anahitaji kukariri majina ya watumiaji na nywila kadhaa. Hii inaweza kuwa ngumu isipokuwa data ya uthibitishaji imeandikwa au kuhifadhiwa kama faili ya maandishi, jambo ambalo linakuwa suala la usalama. Uthibitishaji wa wote unaweza kuondoa tatizo hili bila kuathiri usalama au faragha.

Kumbuka!

Ikiwa una chaguo, chagua programu au kifaa cha uthibitishaji maalum badala ya kupokea misimbo kupitia ujumbe wa maandishi. Ni rahisi kwa mtu anayeshambulia kuelekeza misimbo hiyo kwa simu yao kuliko kuepuka uthibitishaji huo.

2.6.

Mfumo wa Ulinzi wa Ngome

Mfumo wa usalama wa mtandao unaolinda kompyuta kutokana na miunganisho isiyotakiwa kuingia au kutoka kwenye mitandao ya ndani na hasa intraneti, hutumia ngome ambazo zinaweza kutekelezwa kama vifaa vya maunzi au programu, au njia zote mbili zikiwa pamoja. Ngome[117] Inaweza kuwa na kanuni zinazozuia barua pepe zinazoingia au mwingiliano kwenye tovuti fulani. Mfumo wa Ulinzi wa Ngome zinaweza kutumika kama safu ya kwanza ya ulinzi kwa lengo la kulinda kifaa kutokana na kuingiliwa bila idhini. Pia zinaweza kutumia kuzuia watumiaji kufikia mtandao kwa njia fulani.

Ngome kwa vifaa na programu

Ngome zinaweza kuwa vifaa au programu, lakini usanidi bora utajumuisha zote mbili. Mbali na kuzuia ufikiaji usioidhinishwa kwa kompyuta yako na mtandao, ngome pia ni muhimu kwa kuruhusu ufikiaji salama wa mbali kwa mtandao wa kibinafsi kupitia cheti cha uthibitishaji cha salama na mchakato wa kuingia.

Ngome za vifaa za kisasa zinaweza kununuliwa kama bidhaa za kujitegemea, ingawa mara nyingi zinapatikana kama sehemu ya mipangilio ya mtandao kwa upana. Ni muhimu sana kwa usalama wa mfumo wako na miundombinu ya mtandao. Kuta nyingi za vifaa zina njia

117 https://ssd.eff.org/en/glossary/firewall

nne za mtandao au zaidi ambazo zinaweza kuunganisha kompyuta zingine. Kwa mitandao mikubwa zaidi, suluhisho la ngome ya mtandao ya biashara linapatikana.

Ngome za programu zimesakinishwa kwenye kompyuta yako kama programu nyingine yoyote, na unaweza kuzibinafsisha ili uwe na udhibiti fulani juu ya jinsi zinavyofanya kazi na vipengele vyake vya ulinzi. Huduma za ngome za programu zinalenga kulinda kompyuta yako dhidi ya majaribio ya nje ya kudhibiti au kupata ufikiaji wa kompyuta yako usiohalali.

Ngome pia zinaweza kujumuishwa kama sehemu ya mfumo wa uendeshaji wa kompyuta yako. Kwa mfano, Windows Firewall ni programu ya Microsoft Windows ambayo huwajulisha watumiaji kuhusu shughuli za kutiliwa shaka. Programu hiyo inaweza kugundua na kuzuia virusi, minyoo, na washambuliaji ili kuzuia shughuli hatari.

Mbinu za Kuchuja Ngome

Ngome hutumiwa kwa kulinda mitandao za nyumbani na biashara. Programu au vifaa vya kuchuja ngome hufuatilia na kudhibiti taarifa zote zinazoingia kupitia mtandao kuelekea kwenye mfumo wako au mtandao. Kuna mbinu mbalimbali za kuchuja ngome ambazo husaidia kuzuia habari hatari isipenyeze:

- **Kichujio cha Pakiti:** Inachunguza kila pakiti[118] kuingia au kutoka kwa mtandao na inaruhusu au kukataa kulingana na miongozo iliyowekwa na mtumiaji. Uchujaji wa pakiti ni muhimu na wazi kwa watumiaji, lakini inaweza kuwa ngumu kusanidi. Aidha, inakabiliwa na changamoto za uharibifu wa anwani za IP.[119]
- **Mbinu ya maombi::** AInatumia njia za usalama kwa programu maalum, kama vile FTP[120] na Telnet[121] seva. Hii ni nzuri sana, ingawa inaweza kusababisha kupungua kwa utendaji.
- **Lango la kiwango cha mzunguko:** Hutumia njia za usalama wakati wa kutumia TCP[122] au UDP[123] muunganisho umeshaanzishwa. Mara tu muunganisho unapokamilika, pakiti zinaweza kusafiri kati ya wenyeji bila kuhitaji uangalizi zaidi.
- **Seva ya Wakala:**Huchunguza ujumbe wote unaoingia na kutoka kwenye mtandao. Seva ya wakala[124] huficha anwani za kweli za mtandao.

Katika utekelezaji, ngome nyingi hutumia moja au zaidi ya njia hizi kwa pamoja. Ngao hii huchukuliwa kama safu ya mwanzo ya ulinzi katika kuhifadhi habari za kibinafsi. Kwa usalama zaidi, data inaweza kusimbwa kwa njia isiyo ya wazi.

118 https://www.webopedia.com/TERM/P/packet.html
119 https://www.webopedia.com/TERM/I/IP_spoofing.html
120 https://www.webopedia.com/TERM/F/ftp.html
121 https://www.webopedia.com/TERM/T/Telnet.html
122 https://www.webopedia.com/TERM/T/Telnet.html
123 https://www.webopedia.com/TERM/U/User_Datagram_Protocol.html
124 http://ebopedia.com/TERM/P/proxy_server.html

2.7.

Usimbaji fiche

Usimbaji fiche ni mchakato wa kubadilisha taarifa au ujumbe kwa kutumia mchakato wa hisabati (usimbaji), ambapo huonekana kuwa haina maana lakini inaweza kurejeshwa katika hali yake ya awali na mtu au kifaa kinachojua ufunguo sahihi wa kusimbua. Hii inaleta kizuizi kwa watu ambao wanataka kupata maelezo au ujumbe, kwani bila ufunguo sahihi, ni vigumu sana au haiwezekani kurejesha taarifa ya awali. Usimbaji fiche ni sehemu ya mbinu za kryptografia ambazo hulinda usalama wa data.

Usimbaji mwisho hadi mwisho huhakikisha kwamba ujumbe unabadilishwa kuwa ujumbe wa siri na mtumaji wake halisi, na kufahamika tu na mpokeaji wake wa mwisho. Aina nyingine za usimbaji fiche zinaweza kutegemea usimbaji fiche unaofanywa na wahusika wengine. Hii inamaanisha kuwa wahusika hao lazima wawe na uaminifu na maandishi ya awali. Usimbaji mwisho hadi mwisho kwa ujumla huchukuliwa kuwa salama zaidi, kwa sababu inapunguza idadi ya wahusika ambao wanaweza kuingilia au kuvunja usimbaji huo.

2.8.

Mitandao Pepe ya Kibinafsi (VPNs)

VPN ni njia ya kuunganisha kompyuta kwa usalama kwenye mtandao wa shirika lingine au sehemu nyingine ya mtandao. Wakati inapounganishwa kwa VPN, data yote ya kuvinjari wavuti inaonekana kama inatoka kwenye VPN, si kutoka kwa mtoa huduma wa mtandao wa mtu binafsi (ISP).[125] Kutumia VPN huficha anwani ya IP.[126] iliyotolewa na ISP wako kutoka kwa tovuti unazofikia, na kuongeza safu ya faragha. Mbali na kuficha anwani yako ya IP, VPN pia huchakata data yako wakati unapotembelea tovuti.

VPN za kibiashara

VPN ya kibiashara ni huduma ya kibinafsi inayowezesha kutuma kwa usalama mawasiliano yako ya mtandao kupitia mtandao wao wenyewe. Faida ya hii ni kwamba data yako yote unayotuma na kupokea inafichwa kutoka kwa mitandao ya karibu, hivyo kuwa salama dhidi ya wahalifu wa mtandao, ISPs wasioaminika ndani, au mtu yeyote anayepeleleza kwenye mtandao wako wa karibu. VPN inaweza kuwa imewekwa katika nchi ya kigeni, ikilinda mawasiliano kutoka kwa serikali ya eneo hilo na kuepuka udhibiti wa kitaifa. Kwa upande mwingine, trafiki imefichwa kwa VPN ya kibiashara.[127] mwishoni. Hii inamaanisha kwamba ni muhimu kuwa na imani na VPN ya kibiashara (na nchi inayohusika) ili kuhakikisha usalama wa trafiki yako dhidi ya upelelezi. Ingawa VPN ya kibiashara inaweza kudai kutoa “usalama,” hakuna dhamana kamili

125 https://en.wikipedia.org/wiki/Internet_service_provider
126 https://ssd.eff.org/en/glossary/ip-address
127 https://ssd.eff.org/en/glossary/commercial-vpn

ya usalama.

Mifano ya VPN hizi ni CyberGhost VPN,[128] NordVPN,[129] VPN ya Ufikiaji wa Mtandao wa Kibinafsi[130] na TunnelBear (na jaribio la bure la 2GB ya kipimo data).

VPN za bure

VPN ya bure ni huduma inayokupa upatikanaji wa seva ya VPN na programu muhimu bila malipo yoyote. Ingawa VPN hizi zisizolipishwa zinaweza kukusaidia kuepuka gharama, zinaweza pia kuwa na hatari ya usalama kwa sababu zinaweza kuhatarisha udhibiti wa data yako. Kwa mfano, Windscribe VPN ni moja ya huduma za bure ambayo inatoa kikomo cha matumizi ya data kila siku kwa kipindi cha siku 30.[131]

Kumbuka!

Kabla ya kuamua kutumia huduma ya VPN, ni muhimu kusoma maoni ya watumiaji ili kuelewa wasiwasi walionao. Pia, ni vyema kuchunguza sifa ya mtoa huduma wa VPN na kujua anapokoa. Unaweza kutaka kuepuka watoa huduma wa VPN walio katika nchi zinazotiliwa shaka kwa masuala ya usalama.

2.8.

Boresha Usalama Wako Mtandaoni.

Hapa kuna orodha ya tabia za mtandaoni na hatua za usalama za kuchukua ili kusaidia kulinda data yako ya kibinafsi na kuhakikisha uzoefu salama mtandaoni:

- Sasisha mifumo yako na programu.
- Hakikisha una kizuia-virusi kilicho sasishwa kinachoendesha.
- Epuka udanganyifu.
- Tumia nywila lenye nguvu au meneja wa nywila.
- Kuwa makini na viungo unavyo bonyeza; tovuti yenye sifa mbaya inaweza kukufungamanisha na wahalifu mtandaoni na watendaji wabaya.
- Kamwe usiache kompyuta au vifaa vyako bila usimamizi. Funga skrini unapokuwa mbali. Kuacha mfumo wazi ni mwaliko kwa watu wengine kwa data yako.
- Hifadhi data yako kwa uangalifu. Kwa faili za kibinafsi, hakikisha unahifadhi nakala za data yako! Hifadhi wingu na vifaa vya nje ni chaguo nzuri. Pia, simba data yako kabla ya kuihifadhi kwenye kifaa cha nje au wingu.
- Unaponunua mtandaoni au kushiriki data nyeti, hakikisha kuwa unatumia njia ya mawasiliano iliyosimbwa kwa kutafuta “https” au ikoni ya kufunga kwenye upau wa anwani yako.
- Kuwa makini na habari unayoshiriki (na usishiriki) kwenye mitandao ya kijamii.
- Katika maisha ya kimwili, kuwa waangalifu na mashambulizi ya uhandisi wa kijamii, kama ilivyoelezwa hapo juu.
- Hakikisha unafuatilia akaunti zako za kifedha na mitandao ya kijamii kwa shughuli zisizo za kawaida.

128 https://www.cyberghostvpn.com/en_US/
129 https://nordvpn.com/
130 https://www.privateinternetaccess.com/pages/techradar
131 https://windscribe.com/

Vidokezo vya Usalama Mtandaoni eneo la Kazi

Kufanya kazi kutoka nyumbani (telecommuting), kwa sababu yoyote ile, huja na changamoto zake za vitisho vya usalama wa kimtandao. Kazi za kimtandao imepata umaarufu wakati watu na biashara wanatumia teknolojia kutekeleza shughuli kwa mbali.

Hapa kuna orodha ya mwongozo wa usalama wa kufanya kazi kwa mbali:

Vidokezo kwa Wafanyakazi wa Mtandaoni

- Tumia Wi-Fi unayoiamini tu. Kwa muunganisho usio salama, watu walio karibu wanaweza kupeleleza trafiki yako.
- Kwa mitandao ya nyumbani, hakikisha unaficha uhusiano kati ya vifaa vyako na router ya Wi-Fi kwa kusimbwa, kama vile kutumia njia ya kusimbwa ya WEP.[132]
- Tumia vifaa rasmi vya kampuni yako.
- Hakikisha programu ya kinga ya virusi inasasishwa mara kwa mara.
- Sasisha mara kwa mara programu zote na mfumo wa uendeshaji.
- Kumbuka kufanya nakala rudufu ya data yako mara kwa mara. Ni muhimu kuhifadhi faili muhimu kwa ufanisi. Katika hali mbaya, wafanyakazi wanaweza kukumbwa na tatizo la ransomware ambapo data yote inapotea bila nakala rudufu.
- Hakikisha unatumia muunganisho salama kwenda kwenye mazingira yako ya kazi. Hii inajumuisha kutumia VPN au njia nyingine salama kama Teamviewer.
- Kuwa makini na barua pepe za udanganyifu (phishing). Jihadhari na barua pepe zinazohitaji ukaguzi au upyaishaji wa vibali vyako, hata zikiwa zinaonekana kutoka vyanzo unavyoviamini. Thibitisha uhalali wa maombi yoyote muhimu au ya shaka kupitia njia mbadala; epuka bonyeza viungo vya shaka au ufungue viambatisho vya shaka.

Vidokezo kwa Waajiri

- Jielekeze katika kusimamia mifumo inayowezesha ufikiaji wa mbali, kama vile VPN. Hakikisha mifumo hii imeboreshwa kabisa, Ngome zimeundwa vizuri, na programu za kinga dhidi ya zisizo na programu hasidi na kuzuia uvamizi zimewekwa.
- Kamwe usiweke wazi itifaki ya eneo la kazi la Mtandaoni (RDP) moja kwa moja kwenye mtandao (unganisha kwanza kwenye VPN).
- Tumia uthibitishaji wa hatua mbili popote inapowezekana.
- Zingatia kizuizi cha ufikiaji kwenye mifumo nyeti kama inavyostahili.
- Tuma barua pepe za kuwajulisha wafanyakazi wako kuhusu ufahamu wa udanganyifu wa kimtandao (phishing).
- Matumizi ya programu isiyo ruhusiwa kwa madhumuni rasmi (inayoitwa teknolojia ya habari ya kivuli) yanaweza kuongezeka wakati wa kufanya kazi kwa mbali, hivyo kuongeza hatari za usalama na faragha. Hakikisha wafanyakazi wanatambua sera, majukumu ya faragha, na kisheria yanayohusu habari za shirika lako.
- Angalia mipango yako ya kushughulikia matukio ya dharura na, ikiwa ni lazima, zifanyie marekebisho kuzingatia wafanyakazi wanaofanya kazi kwa mbali.
- Pitia mipango yako ya kudumu ya biashara na mipango ya dharura. Hakikisha kuwa hizi ziko za kisasa.

Mkutano wa Video

132 https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

Kutokana na kuenea kwa mikutano ya video tangu wakati wa COVID, kumeshuhudiwa ongezeko la “Mashambulizi kwenye Zoom”, ambapo watu wenye nia mbaya waliingilia mikutano na kusababisha usumbufu kwenye simu za mkutano.

Ili kuzuia matukio kama haya, vidokezo vifuatavyo vinabainisha hatua za kuchukua:

- Hakikisha washiriki wanaweza kujiunga kwa mwaliko tu.
- Hitaji kutumia nywila ili kujiunga na mkutano.
- Washa idhini ya msimamizi kabla ya mtu kujiunga na mkutano.
- Epuka kuchapisha viungo vya mikutano kwenye mitandao ya kijamii.
- Hakikisha programu za mikutano ya video na mazungumzo zinasasishwa mara kwa mara.

Zana za Mikutano ya Video

- Zoom[133]
- Google Meet[134]
- Microsoft Teams[135]
- WhatsApp[136]
- Signal[137]
- Jitsi[138]
- Cisco Webex[139]

2.10.

Zana za Usalama na Haki za Kidijitali

Zana ya Haki za Kidijitali ya Ayeta[140]

Zana shirikishi huelimisha watu kuelewa na kutambua hatari za usalama za kidijitali, kuweka malengo ya usalama, kujifunza jinsi ya kuwa salama mtandaoni na kuwapa nywila iliyotengenezwa.

Ngao ya mrejesho[141]

Zana ya mtandaoni inayosaidia watetezi wa haki za binadamu kubadilisha hali kwa kurekodi unyanyasaji na kufichua uovu.

Ripoti[142]

Mfumo unaokuwezesha kuripoti ukiukaji wa haki za kidijitali. Ripoti imejitolea kulinda kanuni za uhuru wa kidijitali.

Kuram[143]

Tovuti ya kukabiliana na unyanyasaji wa kijinsia mtandaoni (OGBV) iliyoundwa ili kutoa njia kwa wanawake na makundi mengine yaliyo hatarini kuripoti visa vya unyanyasaji wa kidijitali unaofanywa dhidi yao.

133 https://zoom.us/
134 https://workspace.google.com/products/meet/
135 https://www.microsoft.com/en-us/microsoft-teams/group-chat-software
136 https://www.whatsapp.com/
137 https://www.signal.org/
138 https://jitsi.org/
139 https://www.webex.com/
140 https://paradigmhq.org/ayeta/game.html
141 https://feedshield.africa/en/
142 https://ripoti.africa/
143 https://kuramng.org/

SURA 03 | KUPUNGUZA TISHIO

3.1.

Usalama wa Kidijitali na Kimwili

Usalama wa Kidijitali nyakati za Maandamano

Wakati mwingine katika kazi zao, mabingwa wa haki za kidijitali mara nyingi wanashiriki katika maandamano ili kuhakikisha sauti zao zinasikika. Hata hivyo, kubeba vifaa vya kidijitali katika maandamano haya kunaweza kuwa hatari kwa sababu vyombo vya dola vina uwezo wa kutumia zana za uchunguzi wa kidijitali kama vile minara bandia ya simu na teknolojia ya kutambua uso. Teknolojia hizi zinaweza kutumiwa kutambua na kufuatilia waandamanaji, na hivyo kuhatarisha faragha na usalama wao. Kabla ya kushiriki katika maandamano ya amani, waandamanaji wanapaswa kuchukua hatua za kuhakikisha

faragha yao ya kidijitali. Hapa kuna mambo muhimu ya kuzingatia.

Maandalizi ya maandamano kwa siri

Kuwa na VPN ya kuaminika inaweza kusaidia waandamanaji kujificha katika mtandao wao. Vinginevyo, wanaweza kutumia zana kama kivinjari cha Tor ,[144]ambayo huficha shughuli za mtandaoni za mtumiaji kwa kuzuia wachunguzi na kusimba trafiki ya mtandao mara kadhaa. Pia ni muhimu kuhakikisha mipangilio inayohusiana na maandamano inafanywa kupitia programu zilizosimbwa kuanzia mwanzo hadi mwisho badala ya kutumia ujumbe wa maandishi wazi (ambao hujulikana kama SMS).

Kusimbwa Kikamilifu kwa Diski za Vifaa vya Kidijitali

Iwapo kifaa chako kitachukuliwa na maafisa wa sheria, au kikipotea au kuibiwa, kusimbwa kikamilifu kwa diski nzima kunaweza kusaidia kulinda data iliyohifadhiwa kwenye kifaa chako. Android[145] na iOS[146]Vifaa vimeboreshwa na uwezo wa kusimbua diski nzima. Ni muhimu kulinda vifaa hivi kwa kutumia nywila yenye nguvu ili kuzuia upatikanaji usioidhinishwa kwa njia ya nguvu.

Sakinisha Signal

Signal ni programu inayopatikana kwenye iOS[147] na Android[148] ambayo hutoa usimbaji fiche thabiti kutoka mwanzo hadi mwisho ili kulinda ujumbe wa maandishi na simu za sauti. Mbali na usimbaji fiche wa mawasiliano ya mmoja-mmoja, Signal inaruhusu mazungumzo ya kikundi yaliyosimbwa kwa njia fiche. Programu pia hivi majuzi iliongeza kipengele cha kutuma ujumbe unaotoweka popote kutoka sekunde 10 hadi wiki nne baada ya kusomwa kwa mara ya kwanza. Tofauti na huduma zingine kama SnapChat, ujumbe huu wa muda mfupi hautahifadhiwa kwenye seva yoyote na huondolewa kwenye kifaa chako baada ya kutoweka.

Hifadhi data zako

Chukua hatua za tahadhari ili kupunguza hasara zinazoweza kutokea ikiwa kifaa chako kitapotea, kuibiwa, au kuchukuliwa na maafisa wa sheria.Hifadhi nakala za data yako mara kwa mara na uzihifadhi mahali salama ili kuepuka matatizo ya baadaye.

Simu ya Muda

Kwa waandamanaji wanaohofia simu zao kufuatiliwa, njia bora ya muda itakuwa kupata simu ya muda (Simu ya Muda), kifaa cha malipo ya kabla kilichonunuliwa kwa pesa taslimu na kutumika kwa mawasiliano wakati wa maandamano ya amani. Simu za Muda

144 https://www.torproject.org/
145 https://source.android.com/security/encryption/full-disk.html
146 https://www.apple.com/business/docs/iOS_Security_Guide.pdf
147 https://ssd.eff.org/en/module/how-use-signal-ios
148 https://ssd.eff.org/en/module/how-use-signal-android

zinaweza kuwa na faida kwa watumiaji kwa kuwasiliana na watu, hasa wakati wa matukio ya hatari, bila kufichua data yote kwenye simu zao za kawaida. Vinginevyo, kuweka simu yako katika hali ya ndege kunaweza kutumika kwa lengo kama hilo.[149]

Usalama wa Kimwili

Vitisho vya kimwili kwa wanaharakati wa haki za kidijitali ni sawa na vitisho vya usalama wa kidijitali. Vitisho hivi vinaweza kujumuisha kukamatwa, kunyanyaswa, kunyang'anywa vifaa, na kuwekwa kizuizini na maafisa wa serikali. Hii inawaweka katika hatari kubwa na kuhatarisha usalama wao. Ili kupunguza vitisho vya kimwili, wanaharakati wa haki za kidijitali wanapaswa kuwa macho kwa dalili za vitisho kwa usalama wao binafsi kwa kuzingatia mazingira yao, sheria, na watu wanaowazunguka. Kanuni kuu ni kwamba ili mtetezi wa haki za kidijitali aweze kuwalinda wengine, usalama wake mwenyewe lazima uhakikishwe.

3.2.

Kupunguza Vitisho vya Usalama wa Kimwili

Ili kupunguza hatari, wanaharakati wa haki za kidijitali wanashauriwa kuzingatia mambo yafuatayo:

Kubali hatari: Mhathiriwa anayehitaji ulinzi anatakiwa kufahamu kuwa anaweza kuwa katika hatari anapokuwa akifanya shughuli zake.Kwa kuelewa hivyo, mtu huyo anatarajiwa kuchukua hatua za kupunguza hatari au uwezekano wa kukumbana na hatari. Kwa mfano, unapokwenda kufanya kazi za kibinadamu katika eneo la vita, ni muhimu kutambua kwamba usalama wako uko hatarini; kwa hivyo, unahitaji kuwa tayari kukimbia inapobidi, kupiga simu kwa usaidizi, na kuwasiliana na kuelezea dhamira yako kwa wapiganaji wanaohusika katika mapigano ili wakuruhusu kufikia eneo hilo. Vilevile, unapofahamu kuwa data yako inaweza kuwa hatarini kutokana na mashambulizi ya mtandao, unahitaji kuunda nywila imara, kuthibitisha uaminifu wa majukwaa ya kidijitali unayopanga kutumia, kushiriki data yako na watu unaowaamini, na pia kuhifadhi data yako kwenye vifaa mbalimbali vya kuhifadhi.

Epuka hatari:Kujua hatari ni jambo moja na kuepuka ni jambo jingine. Unapojifunza juu ya hatari, unahitaji kuepuka kwa njia zote; huhitaji kudai haki au mamlaka wakati huo. Ili kuepuka hatari, mawasiliano na matendo yako yanapaswa kuwa makini na kubadilika kulingana na hali unayojikuta. Ni muhimu kuzingatia lugha ya mwili wako na kutumia maneno yako kwa busara. Kabla ya kuanza shughuli au kujihusisha na watu, ni lazima kufanya tathmini ya mazingira ili kuelewa kama kuna hatari inayoweza kutokea au la. Hatimaye, ikiwa utathibitisha kuwa wewe ni mlengwa, ni muhimu kujibu kwa kujiamini ili kujilinda dhidi ya mshambuliaji wako.

149 https://ssd.eff.org/en/module/attending-protest

Toa maoni yako kwa watu walio sahihi. Itikadi yako inaweza kuwa na hatari unapoitangaza. Kama mtetezi wa haki za binadamu, ni muhimu kujua ni nani unayeweza kumwambia au kushirikiana nao, kwani si kila mtu atakayekubaliana na maoni yako.

Nyaraka za kibinafsi na za shirika: Kama msemaji wa shirika au mwakilishi wake katika mazingira ambayo huenda si salama, ni muhimu kuwa na ufahamu kamili kuhusu utambulisho wako, majukumu yako, na watu unaowawakilisha. Ushahidi kama huo huwa muhimu sana katika kesi ambapo unaweza kuwa chini ya ulinzi kama mshukiwa. Maranyingi, jinsi unavyojitambulisha, msimamo wako, na shirika lako huwa na athari kubwa juu ya jinsi utakavyoshughulikiwa na watekaji wako.Maranyingi, washukiwa wasio na hatia huachiliwa baada ya kujiwasilisha ipasavyo. Ni muhimu kusimamia lugha ya mwili, uchaguzi wa maneno, na utulivu vizuri wakati wa kukamatwa na wakati wa uchunguzi.

Ufahamu wa hali/mazingira: Wakati unapokutana na changamoto, ni muhimu kuwa makini na mazingira yako, kuzingatia wajibu wako, mahali ulipo, na kujua ni akina nani wapinzani wako. Haya ni mambo muhimu ya kutilia maanani katika hali ngumu ili kuhakikisha usalama wako. Kwa mfano, mtetezi wa haki za binadamu hawezi kuwa katika makambi ya kijeshi na kulaani vitendo vya ukatili vinavyofanywa na askari.

Epuka maeneo ya hatari: Maeneo kama vile mipaka ya miji, sehemu zenye umati mkubwa wa watu, benki, maeneo yenye msongamano wa magari, mikusanyiko ya watu, na maeneo yenye migogoro au vita ni hatari, na ni muhimu kuzingatia nyakati sahihi za kutembelea maeneo hayo kulingana na taaluma na nafasi yako.Kwa mfano, mwanaharakati wa haki za binadamu hashauriwi kuzuru maeneo yenye migogoro bila uhakika wa usalama kutoka kwa wapiganaji.Kwa mfano, katika maeneo ya Anglophone ya Kameruni ambapo kuna mzozo kati ya wapiganiaji wa kujitenga na vikosi vya serikali, wafanyakazi wa misaada ya kibinadamu hawawezi kufikia maeneo ya mapigano bila kuhakikishiwa usalama na pande zote za mzozo. Hii ni kwa sababu wanaweza kuathiriwa na risasi zilizopotea, kukamatwa, au kutekwa nyara ikiwa hawana uhakikisho wa usalama kutoka kwa wapiganiaji.

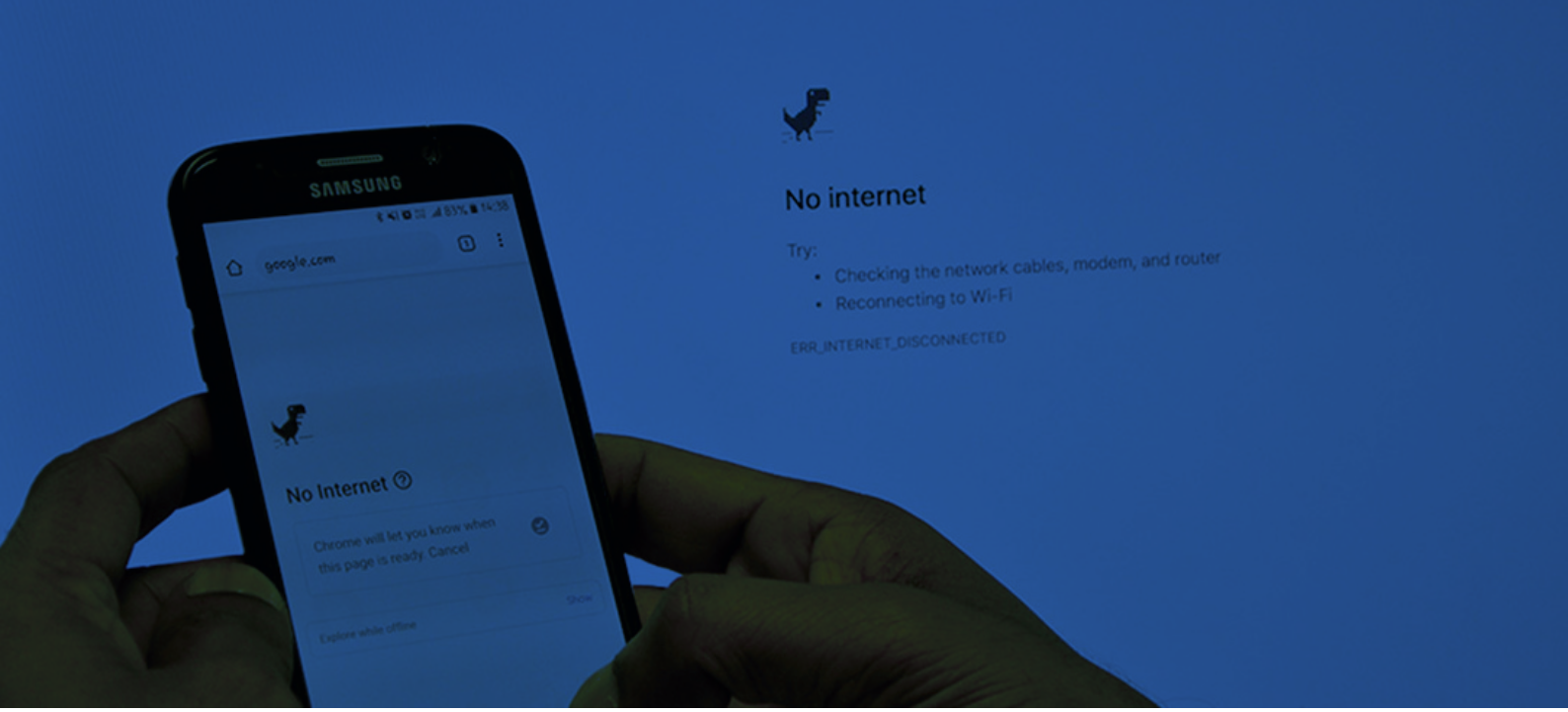
Mavazi: Ni muhimu kuwa na ufahamu wa jinsi unavyoonekana na kuelewa ni vipi unavyopaswa kuvaa wakati unapotekeleza shughuli za kibinadamu. Kwa mfano, wakati unapotoka kufanya kazi shambani, ni muhimu kuvaa viatu vizito na nguo rahisi ambazo unaweza kuepuka au kukimbia haraka ikiwa kuna haja. Ikiwa eneo lako halina usalama wa kutosha, epuka kuvaa mavazi ya thamani kubwa kwani yanaweza kuvutia wizi au mashambulizi kutokana na jinsi unavyoonekana.

Usipingane kwa mtutu wa bunduki au kwenye kambi ya jeshi: Wakati unapokamatwa, kutekwa nyara, au kuzingirwa, fanya chochote unachoelekezwa ili kulinda maisha yako. Usijaribu kupinga na weka kipaumbele cha juu kwa usalama wako.

Kuwa tayari kwa kila kitu: Kabla ya kuanza misheni yoyote, tathmini hatari zinazoweza kutokea na jipange kwa kuchukua vifaa vya huduma ya kwanza na mahitaji muhimu kulingana na afya yako, mazingira ya safari, hali ya hewa, na mahitaji ya kifedha, ili kuhakikisha usalama wako wa kimwili.

Daima kuwa na mawasiliano ya kuaminika. Katika shughuli zenye hatari kama harakati za haki za binadamu, unahitaji kujiandaa kwa hatari ya kukamatwa, kutekwa nyara au mashambulizi kwenye data yako. Kama hatua ya kupunguza hatari, unahitaji kuwa na angalau mwenzako mmoja aliye na uaminifu ambaye unaweza kushirikiana naye kwa kutoa taarifa zako, marudio yako, muda unaotarajiwa kuwepo huko, muda unaotarajiwa kurejea, na hatua zinazopaswa kuchukuliwa iwapo kutatokea dharura.

Nambari za dharura na ufuatiliaji: Hifadhi mawasiliano ya polisi, huduma ya ambulensi, huduma ya moto, hospitali, n.k. mahali salama. Pakua na usakinishe programu ambazo zinaweza kufuatilia kifaa chako unapokuwa katika hatari.



SURA

04 KUZIMWA KWA MTANDAO

Ibara ya 19 ya Azimio la pamoja la za Haki za Binadamu inahakikisha kila mtu haki ya uhuru wa mawazo na kutoa maoni; haki hii ni pamoja na uhuru wa kushikilia maoni bila kuingiliwa na uhuru wa kutafuta, kupokea na kusambaza habari na mawazo kupitia vyombo vyovyote vya habari na bila kujali mipaka. Hata hivyo, miaka ya hivi karibuni kumekuwa na ongezeko la mataifa ya Afrika kutumia njia za kuzuia upatikanaji wa habari mtandaoni. Hii imesababisha mtandao kuwa eneo lenye mchanganyiko zaidi, na visa vya changamoto kwa wanaharakati, walinzi wa haki za binadamu, wapinzani, na waandishi wa habari vimeripotiwa kuongezeka.

Serikali za kiimla zimejikita katika kutumia zana na mikakati ya kidigitali kama vile kuzimwa kwa mtandao, ukandamizaji wa mtandaoni, na upelelezi wa kidigitali ili kukandamiza uhuru wa kutoa maoni. Kulingana na Access Now, mwaka 2022, angalau nchi 35 zilizima

AYETA: ZANA YA HAKI ZA KIDIJITALI 5

mtandao angalau mara 187.[150] Hadi sasa hii ni idadi kubwa kabisa iliyowahi kurekodiwa katika mwaka mmoja mmoja. Mwaka 2023, ifikapo mwezi Septemba, angalau kuzimwa kwa mtandao kumetokea mara 12 katika Afrika Kusini mwa Jangwa la Sahara, hali ambayo imezuia uhuru wa kutoa maoni na kikwazo cha kupata habari, hususan wakati wa uchaguzi na maandamano ya umma.[151] Kwa gharama ya dola milioni 200. Kwa jumla, kuzimwa kwa mtandao kimataifa kulileta gharama ya jumla ya dola bilioni 10 mwaka 2022.[152]

Zaidi, ripoti ya Paradigm Initiative ya mwaka 2019[153] Ripoti ya Paradigm Initiative ya mwaka 2019 ilifunua kuwa baadhi ya serikali za Afrika zimekuwa zikizima mtandao kwa sababu za kisiasa, zinapitisha sheria kali za maudhui mtandaoni, na/au kutumia mashambulizi ya programu hasidi kwa lengo la kulenga walinzi wa haki za binadamu. Ripoti ya PIN Londa ya mwaka 2023 ilionyesha kuwa kati ya nchi 26 zilizo ripotiwa, tano zilizima mtandao.[154] Ripoti iliongeza kuwa uuzaji wa mifano ya Kichina na Kirusi ya mbinu za “utawala wa sheria” kuelekea udhibiti wa mtandao umesababisha udhibiti mkali wa serikali na uvunjaji wa haki za kidigitali kupitia sheria ambazo zinadaiwa kuandikwa kwa lengo la kukuza sheria na utaratibu katika jamii za Kiafrika.

Kuzimwa kwa mtandao kumekuwa na athari mbaya za kiuchumi katika nchi husika. Utafiti wa Deloitte[155] unaonyesha kwamba kwa nchi iliyoshikamana vizuri, athari ya kila siku ya kuzimwa kwa muda mfupi wa mtandao na huduma zake zote itakuwa wastani wa dola milioni 23.6 kwa watu milioni 10. Mwaka 2023, kuzimwa kwa mtandao bado kunasababisha gharama kubwa, na nchi kama Ethiopia ikipoteza takriban dola bilioni 1.59.[156] Hata hivyo, gharama jumla ya kuzimwa kwa mtandao mwaka 2023 ilipungua kwa 67% ikilinganishwa na mwaka 2022, lakini iliongezeka kwa 45% ikilinganishwa na mwaka 2021. Muda wa kuzimwa uliongezeka kwa 18% ikilinganishwa na mwaka 2022, na ongezeko kubwa la 71.5% ikilinganishwa na mwaka 2021.[157]

Licha ya jitihada hizi za serikali mbalimbali za kudhibiti nafasi za kidigitali na hivyo kuzuia kazi ya wale wanaotetea haki za binadamu/haki za kidigitali, zana kadhaa za utambulisho na mzunguko wa mtandaoni kama VPNs na wakalimani mtandao zinatoa matumaini kwa watetezi wa haki za binadamu, walinzi wa haki za kidigitali, waandishi wa habari, na watoa taarifa.

150 https://www.accessnow.org/press-release/keepiton-internet-shutdowns-2022-africa/
151 https://rsf.org/en/how-internet-shutdowns-undermine-journalism-sub-saharan-africa
152 https://technext24.com/2022/12/14/internet-shutdowns-cost-sub-saharan-africa/
153 http://paradigmhq.org/download/dra19/
154 https://paradigmhq.org/londa/
155 https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/the-economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html
156 https://www.forbes.com/sites/emmawoollacott/2024/01/04/government-internet-shutdowns-bring-huge-economic-costs/?sh=557e1b654e44
157 https://www.forbes.com/sites/emmawoollacott/2024/01/04/government-internet-shutdowns-bring-huge-economic-costs/?sh=557e1b654e44

4.1.

Kukwepa vikwazo vya kuzimwa kwa mtandao na ukandamizaji

Mtandao Binafsi wa Kibinafsi (VPN)

Kama ilivyozungumziwa katika sura II kuhusu usalama wa kidijitali, VPN ni njia ya kuunganisha kifaa chako kinachounganishwa na mtandao kwa usalama kwenye mtandao wa shirika lingine kwenye mtandao.Unapotumia VPN, mawasiliano yako yote ya mtandaoni yanafungwa pamoja, yanasimbwa kwa njia fiche, kisha yanatumwa kwa shirika hilo, ambako yanatenguliwa, kufunguliwa, na kisha kutumwa kwenye marudio yake. Kwa mtazamo wa mtandao wa shirika hilo, au kompyuta yoyote kwenye mtandao mpana, inaonekana kama ombi kutoka kwa kompyuta yako linatoka ndani ya shirika hilo, sio kutoka eneo lako. VPNs hutumiwa na watu binafsi ili kukwepa ukandamizaji wa ndani, au kushinda ufuatiliaji wa ndani.

Kivinjari cha Tor

Tor[158] ni programu huria na ya bure inayowezesha mawasiliano ya siri. Jina limetokana na kifupi cha mradi wa asili wa programu “The Onion Router”. Tor ina vipengele vilivyojengwa ndani vinavyokulinda dhidi ya ufuatiliaji wa wavuti, upelelezi, na utambuzi wa vidole mtandaoni.

DuckDuckGo

Ni injini ya utafutaji mtandaoni inayosisitiza kulinda faragha ya watumiaji na kuepuka upendeleo wa matokeo ya utafutaji yaliyo ambatanishwa na tabia za mtumiaji. DuckDuckGo[159] inaji tofautisha na injini nyingine za utafutaji kwa kutoweka wasifu wa watumiaji wake na kwa kuwaonyesha watumiaji wote matokeo ya utafutaji sawa kwa neno moja la utafutaji.

Kubadilisha Mipangilio ya Mfumo wa Majina ya Vikoa (DNS)

Unapokumbana na uchafuzi/udanganyifu wa DNS,[160] Mara nyingi hufanywa na watoa huduma za mtandao, kubadilisha mipangilio ya DNS kunaweza kusaidia kukwepa udhibiti wa DNS. Serikali wakati mwingine ziko mstari wa mbele katika kuendeleza uchafuzi wa DNS ili kuzuia maudhui ambayo raia wake wanaweza kufikia.

4.2.

Kupima Kuzimwa kwa Mtandao na Udhibiti

Chombo cha Uchunguzi wa Uangalizi wa Kuingilia Kati kwenye Mtandao (OONI)

OONI ni mradi huria wa programu ambao lengo lake ni kuimarisha juhudi zisizo jitegemea katika kuongeza uwazi wa ukandamizaji wa

158 https://www.torproject.org/download/
159 https://duckduckgo.com/
160 https://www.fortinet.com/resources/cyberglossary/dns-poisoning

mtandao ulimwenguni kote. OONI inaendeleza programu huria na ya chanzo wazi[161] inayoitwa OONI Probe ili kugundua.

- Kuzuiliwa kwa tovuti;
- Kuzuiliwa kwa programu za ujumbe wa papo hapo (WhatsApp, Facebook Messenger and Telegram);
- Kuzuiliwa kwa zana za kukwepa udhibiti (kama vile Tor and Psiphon);
- Uwepo wa mifumo (middleboxes) katika mtandao wako ambazo zinaweza kuwa zinahusika na udhibiti na/au ufuatiliaji; na
- Kasi na utendaji wa mtandao wako.

Kwa kuendesha OONI Probe,[162] Unaweza kukusanya data inayoweza kutumika kama ushahidi wa udhibiti wa mtandao kwani inaonyesha jinsi, lini, wapi na nani anayetekeleza. Taarifa kuhusu mwenendo wa udhibiti wa mtandao inaweza kupatikana kwenye jukwaa la matokeo ya udhibiti la OONI.[163]

Uchambuzi wa Kukatika kwa Mtandao na Ufuatiliaji (IODA)

“IODA inachunguza mtandao na kugundua kukatika kwa uunganishaji wa mtandao moja kwa moja kwenye dashibodi ya matatizo ya mtandao[164] ambayo inawezesha watumiaji kufuatilia kukatika kwa mtandao kote duniani kwa wakati halisi.

Maabara ya Vipimo (M-Lab)

M-Lab[165] Inatoa kipimo wazi na kinachoweza kuhakikiwa cha utendaji wa mtandao wa kimataifa. Kupitia M-Lab, watumiaji wanaweza kupima utendaji wa mtandao wao ili kuangalia kasi ya mtandao. Hii husaidia kutambua kupunguzwa kwa kasi ya mtandao.

4.3.

Uhamasishaji Dhidi ya Kuzimwa kwa Mtandao Barani Afrika

Zana ya Gharama ya Kuzimwa kwa Mtandao ya NetBlocks (COST)

Zana mtandaoni inayoendeshwa na data[166] Kwa ajili ya kupima gharama za kuzimwa kwa mtandao, na kuishawishi serikali kudumisha mtandao ukiwa hai. Zana hii inawezesha mtu yeyote - ikiwa ni pamoja na waandishi wa habari, watafiti, watetezi, wapangaji sera, biashara, na wengine wengi - kuhesabu kwa haraka na kwa urahisi gharama za kiuchumi za kuzimwa kwa mtandao, kukatwa kwa data za simu na vizuizi vya mitandao ya kijamii kwa kutumia maelfu ya vigezo vya kikanda kutoka Benki ya Dunia, ITU, Eurostat na Sensa ya Marekani.[167] Ni tovuti ya kimataifa ya uchunguzi wa mtandao inayotoa uchambuzi na ripoti za kupungua kwa kasi ya mtandao, kuzimwa kwa

161 https://github.com/ooni/probe
162 https://ooni.org/install/
163 https://explorer.ooni.org/findings
164 https://ioda.inetintel.cc.gatech.edu/dashboard
165 https://speed.measurementlab.net/#/
166 https://netblocks.org/cost/
167 https://netblocks.org/reports

mtandao na ukandamizaji wa mtandao.

Kampeni ya #WashaMtandao

Kampeni hii ya kimataifa[168] Inasimamiwa na AccessNow na inalenga kuhamasisha serikali ulimwenguni kote kutokuzima mtandao na kuruhusu mtiririko huru wa habari.

Mchezo wa Kuzimwa kwa Mtandao

Shirika la Mawasiliano Kwa Maendeleo (APC) lilianzisha mchezo wa mtandao wa kuzimwa unaoshirikisha washiriki[169] ambao unatoa ufafanuzi kuhusu aina mbalimbali za kuzimwa kwa mtandao na njia za kuyapinga. Mchezo huu unalenga kwa watetezi wa haki za binadamu, umma kwa ujumla na wataalamu wa sheria.

168 https://www.accessnow.org/campaign/keepiton/
169 https://shutdowngame.apc.org/

FAHARASA

Nyongeza- Programu ndogo inayobadilisha programu nyingine kwa kubadilisha jinsi inavyofanya kazi au kile inaweza kufanya. Mara nyingi, vifaa vya nyongeza vinaweza kuongeza sifa za faragha au usalama kwenye vivinjari vya wavuti au programu za barua pepe. Baadhi ya vifaa vya nyongeza ni programu hasidi, hivyo jikinge kwa kusakinisha tu vile vilivyo aminika na kutoka vyanzo rasmi.

Kutokujulikana– Hali ya kutokuwa na utambulisho

Kinga-virusi - Programu ya kuzuia virusi hutumiwa kuzuia, kugundua, na kuondoa programu hasidi, ikiwa ni pamoja na virusi vya kompyuta, minyoo, na farasi wa Trojani. Baadhi ya mifano ya programu za kuzuia virusi ni McAfee, Avast, AVG, na Kaspersky.

Udhibiti - Udukuzi wa Mtandao ni udhibiti au kukandamiza kile kinachoweza kufikiwa, kuchapishwa, au kutazamwa kwenye mtandao, uliofanywa na wasimamizi au serikali.

Kuzunguka – Matumizi ya njia na zana mbalimbali za kudhibiti mtandao

Kriptografia - Sanaa ya kubuni mifumo ya siri ambayo inaruhusu kubadilishana ujumbe na mpokeaji bila wengine kuelewa ujumbe huo.

Usafi wa kidijitali - Inahusu hatua kama vile kuandaa faili kwenye kompyuta yako, kuzilinda akaunti zako za mitandao ya kijamii, kuongeza programu mpya au teknolojia ili kufanya maisha yako ya kidijitali kuwa rahisi au salama zaidi.

Haki za kidijitali - Haki za kidijitali ni haki za binadamu katika enzi ya intaneti.

Usimbaji fiche- Mchakato unaofanya ujumbe uwe usioweza kusomwa isipokuwa na mtu anayejua jinsi ya “kufungua Usimbaji fiche” ili kuurudisha katika hali inayoweza kusomwa.

Ufunguo wa Usimbaji - Kitufe cha kusimbua ni taarifa inayotumiwa kubadilisha

ujumbe kuwa mfumo ambao hauwezi kusomwa. Mara nyingi, unahitaji kitufe kile kile cha kusimbua ili kurejesha ujumbe. Kwa hali nyingine, kitufe cha kusimbua na cha kusimbuana inaweza kuwa tofauti.

Ngome- Chombo ambacho hulinda kompyuta dhidi ya uhusiano usiohitajika kutoka kwenye mitandao ya ndani au ya nje. Ngome inaweza kuwa na kanuni ambazo zinazuia barua pepe zilizotumwa au uhusiano na tovuti fulani. Kizuizi kinaweza kutumika kama safu ya kwanza ya ulinzi ili kulinda kifaa kutokana na uvamizi usiotarajiwa. Pia kinaweza kutumiwa kuzuia watumiaji kufikia mtandao kwa njia fulani.

Itifaki ya Kuhamisha Faili (FTP) - Mfumo wa kawaida wa mtandao unaotumika kuhamisha faili kutoka kwenye seva moja hadi nyingine kupitia mtandao, kwa kutumia Itifaki ya Udhibiti wa Usambazaji, kama vile mtandao wa intaneti.

Kuzima kwa mtandao –Kuzimwa kwa mtandao ni kukatizwa kimakusudi kwa mtandao au mawasiliano ya kielektroniki, na kuyafanya kutoweza kufikiwa au kutoweza kutumika kwa watu mahususi au ndani ya eneo, mara nyingi ili kudhibiti mtiririko wa taarifa.

Anwani ya IP – Anwani ya Itifaki ya Mtandao ndiyo hutambulisha kwa njia ya kipekee vifaa vilivyounganishwa kwenye mtandao.

Programu hasidi - Programu hasidi ni programu zilizoundwa kufanya shughuli zisizotakikana kwenye kifaa chako. Virusi vya kompyuta ni mfano wa programu hasidi. Programu nyingine zinaweza pia kuiba nywila, kurekodi bila idhini yako, au kufuta data yako.

Mfumo wa Uendeshaji (OS)- Programu inayoendesha programu zingine zote kwenye kompyuta au kifaa. Windows, Linux, Android, HarmonyOS na Apple OS X na iOS zote ni mifano ya mifumo ya uendeshaji.

Meneja wa nywila - Zana inayounda na kuhifadhi maneno ya siri ili uweze kutumia nywila nyingi tofauti kwenye tovuti na huduma tofauti bila kulazimika kuzikariri.

Neno la siri - Neno la siri ndefu kuliko neno la siri, ambalo kawaida huwa ni neno moja tu.

Kompyuta (kompyuta ya kibinafsi). - Kompyuta yenye matumizi mbalimbali.

PGP - Pretty Good Privacy ilikuwa moja ya utekelezaji maarufu wa kwanza wa ushifirishaji wa kifunguo cha umma kusaidia wanaharakati na wengine kulinda mawasiliano yao.

Wakala –Programu au kifaa kwenye seva kinachofanya kama mpatanishi kwa maombi kutoka kwa wateja wanaotafuta rasilimali kutoka kwa seva zinazotoa rasilimali hizo. Mfumo wa mwakilishi kwa hivyo hufanya kazi kwa niaba ya mteja wakati wa kuomba huduma, na inaweza kuficha asili halisi ya ombi kwa seva ya rasilimali.

Swali la Usalama- Maswali yanayohusiana na nywila ambayo unatarajiwa kujua majibu yake pekee.

Programu – Neno jumla linalotumika kwa ajili ya programu, maandishi na mipango inayofanya kazi kwenye kifaa.

TCP (Itifaki ya Udhibiti wa Usambazaji) - Kiwango cha mawasiliano kinachowezesha programu za maombi na vifaa vya kuhesabu kubadilishana ujumbe kwenye mtandao.

Telnet (mtandao wa teletype) - Telnet ni itifaki ya maombi ya mteja/seva inayotoa ufikiaji kwa vidhibiti vya simu za mbali za mifumo kwenye mitandao ya eneo la ndani au intaneti.

Tor - Programu huru na ya chanzo wazi inayowezesha mawasiliano ya kujificha. Jina limetokana na kifupi cha jina la mradi wa awali wa programu «The Onion Router».

Uthibitishaji wa Mara Mbili - Uthibitishaji wa Mara Mbili (2FA) ni njia ya kuwaruhusu watumiaji kuthibitisha utambulisho wao kwa mtoa huduma kwa kutumia mchanganyiko wa njia mbili tofauti za uthibitishaji. Hizi zinaweza kuwa kitu ambacho mtumiaji anajua (kama nywila au PIN), kitu ambacho wanamiliki (kama kifaa cha elektroniki au simu ya mkononi), au kitu ambacho kimeunganishwa au kushikamana nao (kama alama za vidole).

URL (Kitambulisho cha Rasilmali cha Kipekee)- Anwani ya ukurasa wa wavuti.

UDP (Itifaki ya Datagram ya Mtumiaji) - Itifaki ya mawasiliano inayotumiwa kwenye intaneti kwa uhamishaji unaohitaji muda mfupi sana, kama vile kucheza video au kutafuta DNS.

Mtandao Binafsi za Kibinafsi – VPN hutumiwa kuunganisha kwenye mtandao kupitia njia iliyosimbwa kwa njia fiche. Mtoa huduma wako wa Intaneti, au mtu yeyote anayenusa kwenye Wi-Fi isiyolipishwa unayotumia kufikia wavuti, anaweza tu kuona muunganisho wako kwenye huduma ya VPN, huku tovuti unayotembelea itarekodi tu muunganisho kutoka kwa seva za VPN. Chaguzi tofauti za VPN zinapatikana, kulingana na kile unachohitaji.[170]